A COMPARISON OF 802.11 WIRELESS TRANSMITTER LOCALIZATION TECHNIQUES

By

KELLEN MITCHELL HARWELL

Bachelor of Science in Electrical Engineering

Oklahoma State University

Stillwater, Oklahoma

2005

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
May, 2008

A COMPARISON OF 802.11 WIRELESS
TRANSMITTER LOCALIZATION
TECHNIQUES

Thesis Approved:

Dr. Keith A. Teague

Thesis Adviser

Dr. George Scheets

Dr. James C. West

Dr. A. Gordon Emslie

Dean of the Graduate College

TABLE OF CONTENTS

Chapter Page

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

Figure Page

Figure Page

CHAPTER 1

INTRODUCTION

Since its standardization, 802.11 wireless networking has experienced rapid growth. Its ease of deployment and low cost makes it an easy choice for many in need of establishing network connectivity. However, during the setup process, many neglect to implement security protocols on the wireless network. This presents a significant security risk, as internal information is exposed to outside listeners. Thus a system is needed to geographically locate these rogue networks so that an administrator can either remove or properly secure it. This problem can become complicated and time consuming for a large facility such as a business complex or government installation, as the propagation environment can vary greatly between sites.

Previous research has focused primarily on indoor asset and personnel tracking techniques that utilize previous knowledge of building layout and access point locations. Using this a priori information, signal strength measurements can be used to create a radio map of the building [8] or formulate a site specific propagation model [9]. While these techniques are effective in locating resources for a particular indoor area, they cannot be applied to large, outdoor areas in which prior structural and network layout information is unknown.

This thesis presents multiple outdoor collection methods used to localize indoor access points. These techniques require no prior knowledge of propagation environment or transmitter location, and can be used to survey a large facility in a timely manner. In terms of accuracy, a comparison is made between range based systems which utilize omnidirectional antennas, and angle of arrival based systems which use directional antennas. For the latter, the relationship between accuracy and antenna directionality is also explored. Collections are performed at several test sites in order to evaluate the performance of each method in varying propagation environments. In order to keep system costs low, hardware is limited to low cost commercial 802.11 equipment and a laptop.

CHAPTER 2

SCOPE

Before describing the various collection and analysis techniques used in this thesis, a set of objectives and operational constraints must first be defined:

This research specifically addresses indoor to outdoor localization, meaning the transmitter is indoors and the collection system is outdoors. Techniques specific to other scenarios such as indoor to indoor estimation are not discussed, as this work has been addressed previously.

These techniques are intended to be applicable to a wide variety of collection sites. Thus prior site specific information, such as architectural, environmental, and network layout, is considered to be unknown.

In order to collect wireless data for large sites in a timely manner, the system utilizes sensors mounted on the roof of an automobile. As such, collection is limited to areas where roads are easily accessible. For non-stationary schemes, driving should be at relatively low speeds to allow a sufficient number of frames to be collected from target access points. For this thesis, a speed of between 15-20 miles per hour was maintained.

CHAPTER 3

LOCALIZATION TECHNIQUES

There are a variety of techniques used for location estimation, each effective when given the right constraints. However, when operating with a limited data set or in an unknown environment, some methods produce undesirable results. This chapter provides background information for the two techniques that are most relevant to this thesis: angle of arrival based estimation and range based estimation. The collection methods specific to this research that utilize these techniques are discussed in chapter 7.

3.1. Angle of Arrival Based Localization

Angle of arrival (AoA) based systems operate by measuring the direction from which a signal is received (methods for determining AoA are discussed in detail later in this section). Upon knowledge of two or more AoA measurements, the intersection of lines technique can be computed to determine the source location.

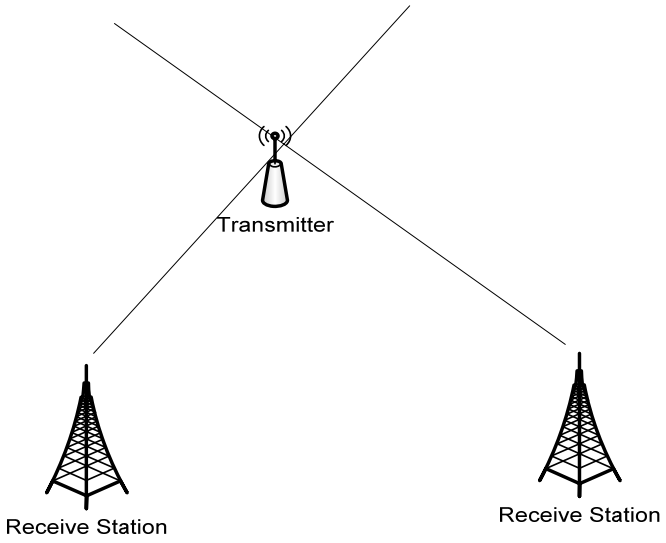

Figure 3.1.1 –Source Estimation Using Two AoA Measurements

For the case of a two receiver system shown in figure 3.1.1, an estimate can be computed because an intersection always exists between two non-parallel lines. This intersection can be computed using the basic equation (eq. 3.1.1) for a line y_i, where m_i is the slope and b_i is the y-axis intercept. Two lines y_0 and y_1 yield a system of linear equations, shown by eq. 3.1.3 through eq. 3.1.5. Solving eq. 3.1.6 produces the coordinates of the intersection p.

$$y_i = m_i x + b_i \qquad \text{eq. 3.1.1}$$

$$-m_i x + y_i = b_i \qquad \text{eq. 3.1.2}$$

$$p = \begin{pmatrix} x \\ y \end{pmatrix} \qquad \text{eq. 3.1.3}$$

$$Ap = B \qquad \text{eq. 3.1.4}$$

$$A = \begin{bmatrix} -m_0 & 1 \\ -m_1 & 1 \end{bmatrix} \qquad \text{eq. 3.1.5}$$

$$B = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} \qquad \text{eq. 3.1.6}$$

$$p = A^{-1}B \qquad \text{eq. 3.1.7}$$

For a system of three or more lines, however, a single common intersection may not always exist. In this case, the least squares method [17] can be used to find an approximate solution in the absence of a common intersection. The formula for solving the least squares approximation is shown in eq. 3.1.8 using the matrices A and B for an overdetermined system.

$$x = (A^T A)^{-1} A^T B \qquad \text{eq. 3.1.8}$$

$$A = \begin{bmatrix} -m_0 & 1 \\ -m_1 & 1 \\ -m_2 & 1 \\ \cdots & \ldots \\ -m_n & 1 \end{bmatrix} \qquad \text{eq. 3.1.9}$$

$$B = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ \cdots \\ b_n \end{bmatrix} \qquad \text{eq. 3.1.10}$$

If confidence levels for particular measurements are known, a weighted least squares calculation can be made in order to to give certain lines more influence in the overall result. In order to achieve this, only a slight modification to the previous equations are necessary, as shown in eq 3.1.11 and 3.1.12.

$$A = \begin{bmatrix} -w_0 m_0 & w_0 \\ -w_1 m_1 & w_1 \\ -w_2 m_2 & w_2 \\ \cdots & \cdots \\ -w_n m_n & w_n \end{bmatrix} \quad \text{eq. 3.1.11}$$

$$B = \begin{bmatrix} w_0 b_0 \\ w_1 b_1 \\ w_2 b_2 \\ \cdots \\ w_n b_n \end{bmatrix} \quad \text{eq. 3.1.12}$$

Figures 3.1.2 and 3.1.3 graphically display equally weighted least squares approximations for overdetermined systems in two dimensional Cartesian coordinate space. The approximate intersection is shown by the transmitter icon.

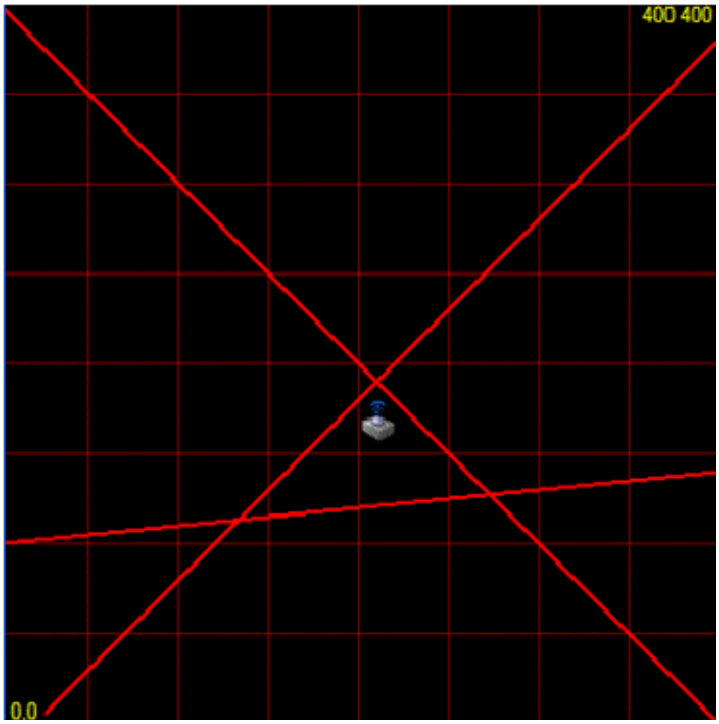

Figure 3.1.2 – Least Squares Approximation – 3 AoA Measurements

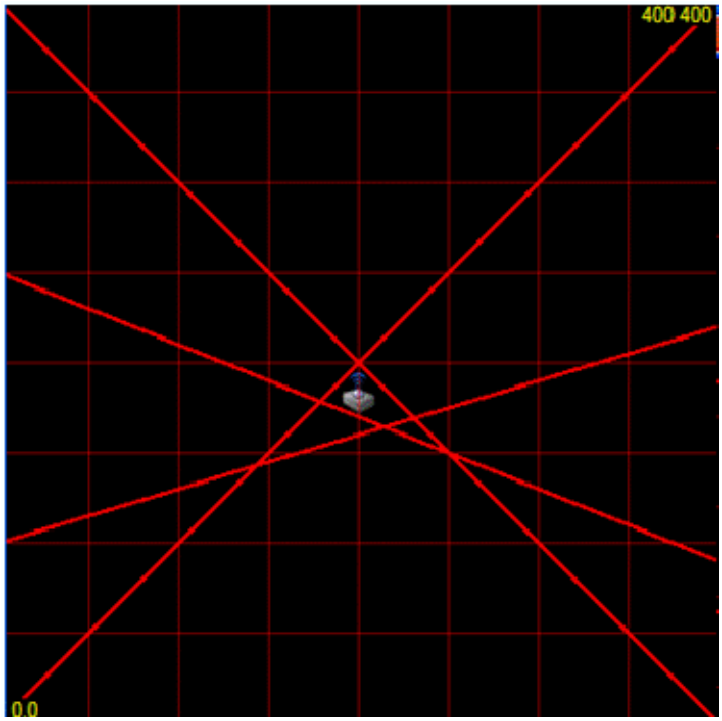

Figure 3.1.3 – Least Squares Approximation - 4 AoA Measurements

The accuracy of AoA systems will improve as the angle between receivers with respect to the source approaches $\pi/2$ or $-\pi/2$. Having this wide angular spacing helps combat small errors in AoA. Figure 3.1.4 shows two receive stations that have low angular spacing with respect to the source. Notice how slight errors in AoA result in a poor intersection estimation. Figure 3.1.5 also shows similar flawed AoA measurements; however, for this case error is minimized due to greater angular spacing between receivers.

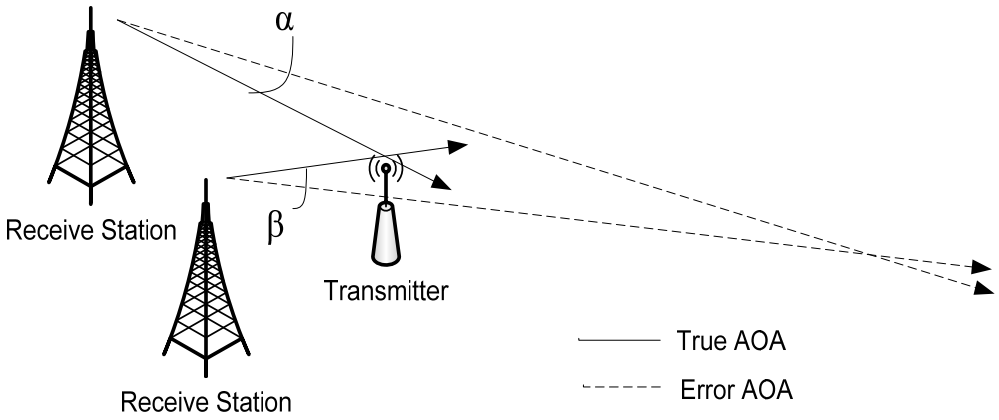

Figure 3.1.4 – Low AoA Angular Spacing

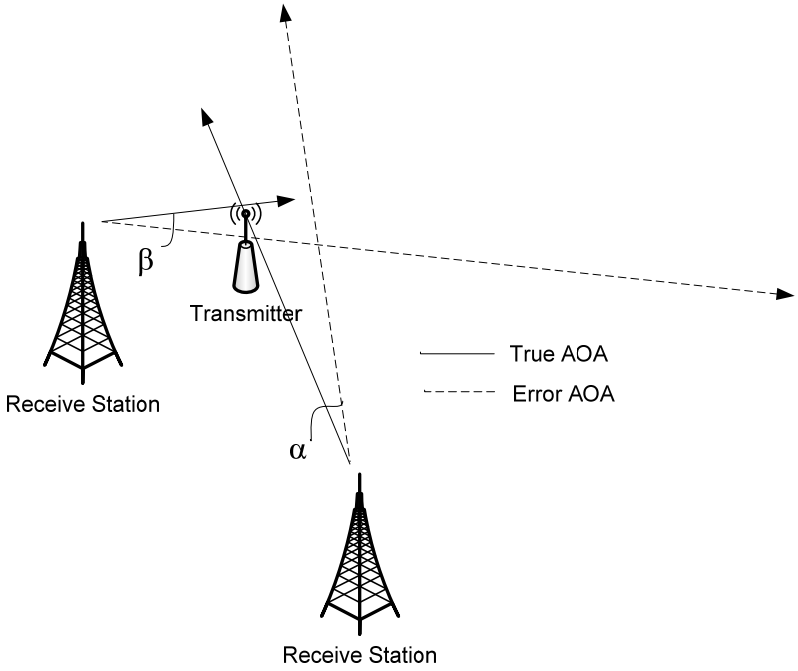

Figure 3.1.5 – Wide AoA Angular Spacing

3.1.1. Directional Antenna Scanning

One method used to determine source angle is by mechanically rotating a directional antenna 360° and storing the direction and magnitude of each received signal. This technique is sufficient when signals are being transmitted with adequate repetition, thus allowing a quasi-uniform sampling rate. It is not sufficient, however, for sources that transmit at irregular intervals. Due to the antenna's gain changing with respect to time, an intermittent signal could effectively be "missed" because of antenna orientation. Antenna sweeping is an inexpensive method for implementing AoA, as it only requires a single antenna and receiver pair. However, it does require some method of updating azimuth orientation, which is typically achieved using an encoder or electronic compass.

3.1.2. Omnidirectional Antenna Array

Another method of determining AoA is by using an array of omnidirectional antennas to measure phase delay between antenna elements. For signals transmitted at irregular intervals, this is a reliable system, as the antenna gain does not change with respect to time. However, due to the speed at which radio signals travel, it is imperative that the system be synchronized and have a high sampling rate. This demand on precise hardware makes omnidirectional arrays an expensive and complex solution. Figure 3.1.6 shows a top view of a 3x3 array which can measure AoA in azimuth.

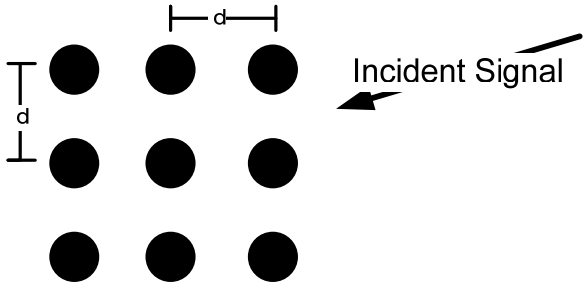

Figure 3.1.6 – 3x3 Onmidirectional Antenna Array

3.1.3. Circular Directional Antenna Array

Multiple directional antennas oriented in a circular pattern can also be used to determine AoA. When a signal of interest is received, the AoA can be quantized to a multiple of $2\pi/N$ angles, where N is the number of antenna elements. Alternately, correlation of signal strength between antenna elements could instead be performed to increase AoA resolution.

A circular array relies on received signal strength measurements rather than precise timing to determine AoA, thus the need for hardware synchronization is eliminated. While this does reduce complexity with respect to 3.1.2, it requires a dedicated receiver for each antenna element, making it more costly than 3.1.1. Figure 3.1.7 shows an array of 8 elements, each spaced $\pi/4$ radians apart.

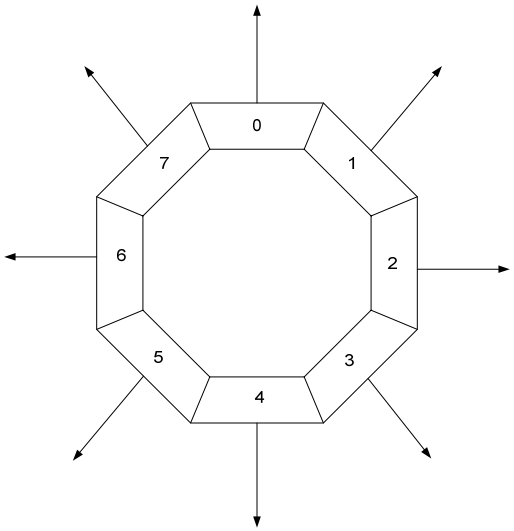

Figure 3.1.7 – 8 Element Circular Array

3.2. Range Based Localization

Range based systems estimate transmitter location using signal strength measurements from multiple receivers of known location. Using RF propagation models, these signal strength values can be used to calculate the distance between transmitter and receiver. This method is used when sufficient knowledge of the wireless system exists, such as transmit power, antenna gains, and loss models. For example, eq. 3.2.1 shows the Friis free-space propagation equation [2], which is often used to calculate range for wireless systems. By rearranging terms (eq. 3.2.2), the range d is easily calculated, where P_r and P_t are transmit and receive power, G_t and G_r are transmit and receive antenna gains, λ is the wavelength, and L is the system loss factor.

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\lambda)^2 d^2 L} \qquad \text{eq. } 3.2.1$$

$$d^2 = \frac{P_t G_t G_t \lambda^2}{(4\lambda)^2 P_r L} \qquad \text{eq. } 3.2.2$$

It should be noted that for range based systems, *N+1* range measurements must exist to solve for *N* unknown axes. With that stated, figure 3.2.1 shows that only the horizontal position can be solved given two range values. Only by adding a third range can a single location be found, as shown in figure 3.2.2.

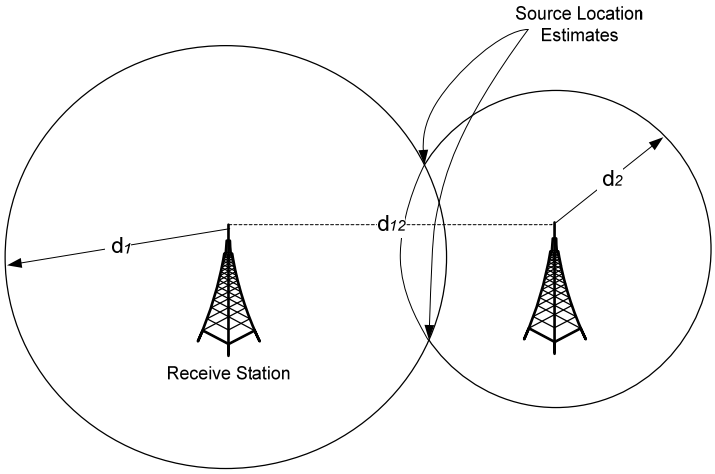

Figure 3.2.1 – Source Estimate Using 2 Range Estimates

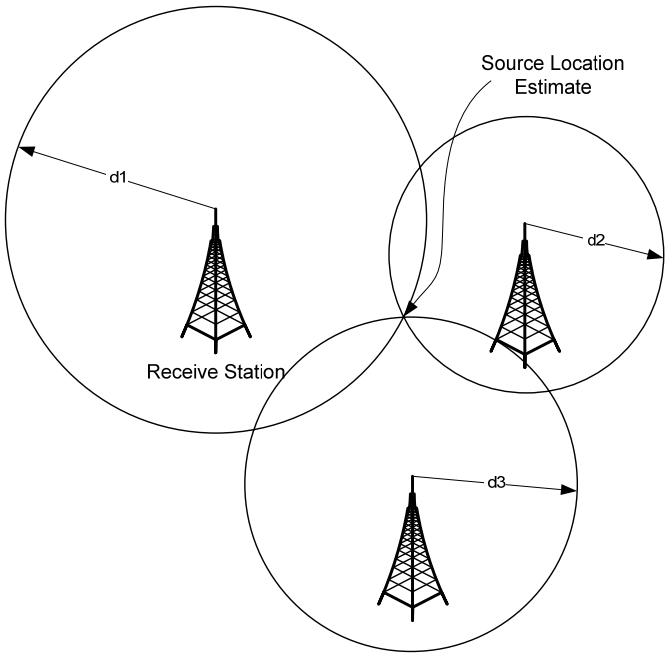

Figure 3.2.2 – Source Estimate Using 3 Ideal Range Estimates

In order for a single intersection to exist, range estimates must produce perfect distances. It is not practical to expect such precision, and thus a scenario similar to figure 3.2.3 is typically produced from inexact range estimates. An approximate intersection for this situation can be found using eq. 3.2.3 and eq. 3.2.4 [5]. By minimizing the estimation error ε_i for ranges (*Ri*) corresponding to points (x_i, y_i) from multiple locations (i = 0, 1, 2…), an optimal intersection estimate $(\overline{x}, \overline{y})$ can be obtained.

$$\varepsilon_i = \mathrm{R}_i - sqrt((x_i - x)^2 + (y_i - y)^2) \qquad \text{eq. 3.2.3}$$

$$(\overline{x}, \overline{y}) = \min_{(x,y)} \sum_{i}^{N} \varepsilon_i \qquad \text{eq. 3.2.4}$$

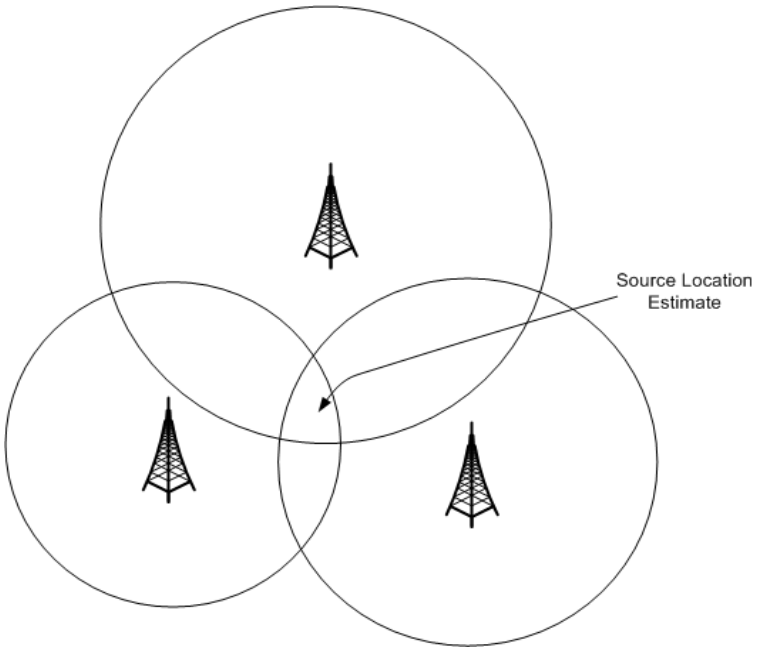

Figure 3.2.3 – Location Estimate Using 3 Realistic Range Estimates

The disadvantage to this method is that a non-linear equation must be solved, which is computationally expensive. This would not be unfeasible if this research were to be implemented in real time. Therefore, an alternative method must be found in order to reduce computational complexity.

In order to find an linear approximation, the process of multilateration [5] using the least squares method can be used. This is achieved by calculating the intersection lines between the ranges and using least squares method to the minimize the distance between them. The intersection line between two ranges is calculated using eq. 3.2.3 through 3.2.5, where receive locations (x_i, y_i) and (x_j, y_j) are distances R_i and R_j from the estimated source location (x, y).

$R_i{}^2 = (x_i - x)^2 + (y_i - y)^2$ eq. 3.2.3

$$R_j^2 = (x_j - x)^2 + (y_j - y)^2 \qquad \text{eq. 3.2.4}$$

$$R_i^2 - R_j^2 \rightarrow 2x(x_j - x_i) + 2y(y_j - y_i) = R_i^2 - R_j^2 - x_i^2 - y_i^2 + x_j^2 + y_j^2 \qquad \text{eq. 3.2.5}$$

By repeating instances of eq. 3.2.5, a system of simultaneous linear equations can be obtained, shown by eq. 3.2.6 through 3.2.9.

$$Ap = B \qquad \text{eq. 3.2.6}$$

$$A = \begin{bmatrix} 2(x_0 - x_1) & 2(y_0 - y_1) \\ 2(x_0 - x_2) & 2(y_0 - y_2) \\ 2(x_0 - x_3) & 2(y_0 - y_3) \\ \cdots & \cdots \\ 2(x_0 - x_n) & 2(y_0 - y_n) \end{bmatrix} \qquad \text{eq. 3.2.7}$$

$$p = \begin{pmatrix} x \\ y \end{pmatrix} \qquad \text{eq. 3.2.8}$$

$$B = \begin{bmatrix} R_1^2 - R_0^2 - x_1^2 - y_1^2 + x_0^2 + y_0^2 \\ R_2^2 - R_0^2 - x_2^2 - y_2^2 + x_0^2 + y_0^2 \\ R_3^2 - R_0^2 - x_3^2 - y_3^2 + x_0^2 + y_0^2 \\ \cdots \\ R_n^2 - R_0^2 - x_n^2 - y_n^2 + x_0^2 + y_0^2 \end{bmatrix} \qquad \text{eq. 3.2.9}$$

Finally, a single location p can be obtained by using the least squares method in eq. 3.2.10.

$$p = (A^T A)^{-1} A^T B \qquad \text{eq. 3.2.10}$$

Figure 3.2.4 shows three ranges along with their corresponding lines of intersection which are used to estimate the source locaton, shown by the transmitter icon.

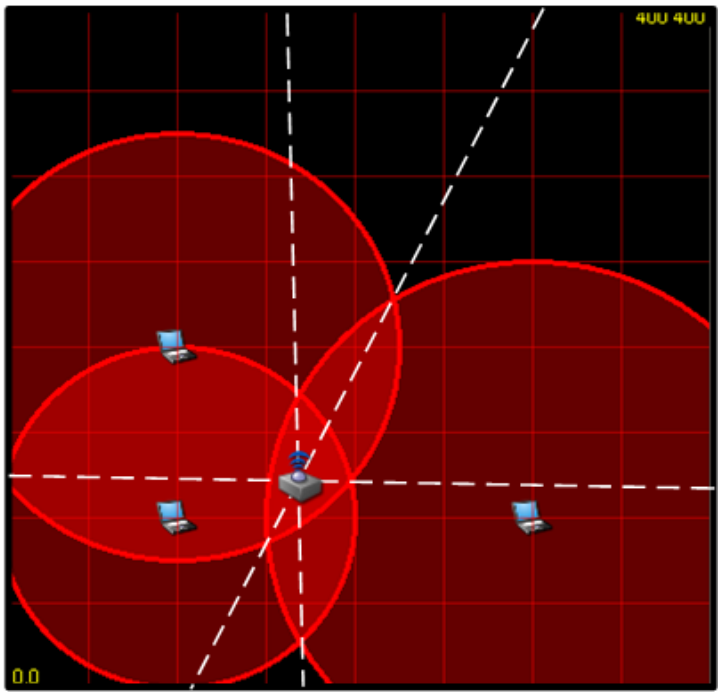

Figure 3.2.4 – Multilateration Using 3 Ranges

An important constraint placed on this calculation is that collection points must not be collinear. Such creates near parallel lines of intersection, which cause estimation errors in the direction perpendicular to the linear path. An example of this is shown in figure 3.2.5, where the center collection point is centered slightly lower than the other points on the vertical axis. This results in lines of intersection which have low angular spacing, resulting in an inaccurate estimation on the vertical plane. Figure 3.2.6 further demonstrates the relationship between collection path linearity and estimation error due to parallel intersection lines.

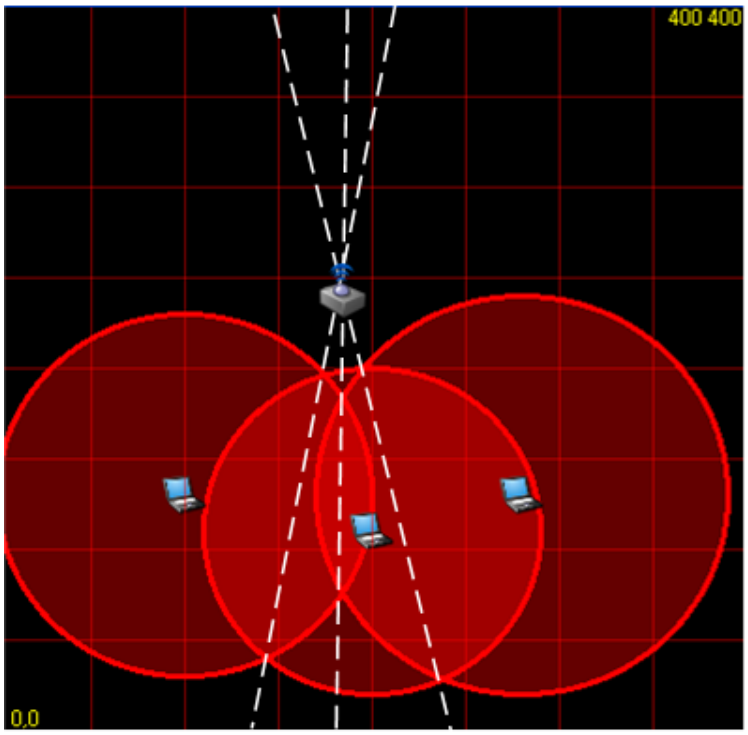

Figure 3.2.5 – Multilateration Inaccuracy Due To Linear Measurements

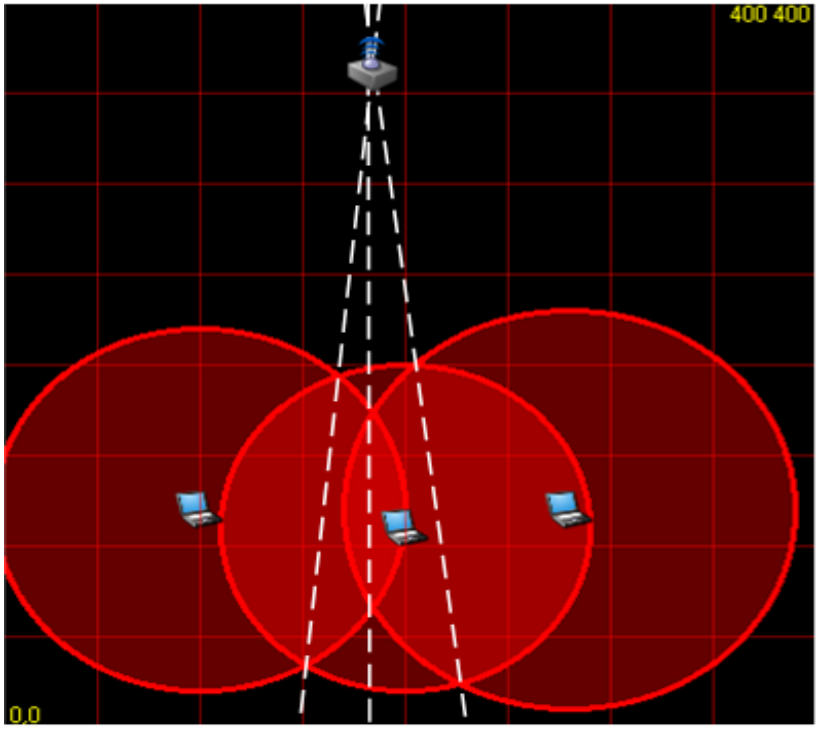

Figure 3.2.6 – Multilateration Inaccuracy Due To Linear Measurements

CHAPTER 4

RF PROPAGATION MODELS

In order to accurately estimate the spatial separation between transmitter and receiver, a propagation model must be used that is suitable to a specific operational environment. However, because mobile collections take place in various types of environments and site specific parameters cannot be included into the model, a general model for path loss must be used.

This chapter discusses the propagation models evaluated by this research. In many cases, the frequency and antenna height constraints of this work contradict those imposed by the models. However, because strict obedience of these restrictions would eliminate most models, the effect of constraint noncompliance for each model is explored.

4.1. Free Space Model

The free space propagation model can be used to describe a communication system that has an unobstructed, line of sight path between the transmitter and receiver. The received power of free space propagation obeys the inverse square law, with each doubling of distance resulting in an additional 6dB of path loss [2]. The Friis free space equation (eq. 4.1.1) describes this, where P_r and P_t are the received and transmitted power in watts, G_t and G_r represent the transmit and receive antenna gains, λ is the wavelength in meters, L is the system loss factor not related to propagation, and d is the separation between the transmitter and receiver in meters.

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\lambda)^2 d^2 L} \qquad \text{eq. 4.1.1}$$

Typically, the free space model is only applicable in a system such as a satellite communication link that has no atmospheric losses. Ground based systems typically have obstructions such as buildings, trees, the earth, etc, which will introduce losses to the signal not representative by free space propagation.

4.2. Log Distance Model

When encountering propagation environments that contain obstructions, path loss can vary greatly based on surroundings. Log-distance path loss, shown by eq. 4.2.1, uses a measured reference path loss $PL(d_0)$ and a path loss coefficient n to describe the average large scale path loss for a given environment. The actual distance between transmitter and receiver for a given reading is d. The distance d_0 chosen to calculate a reference path loss is typically chosen to be 1m or 100m in a low to medium range system. Longer range systems commonly use 1km references [2].

$$PL = PL(d_0) + 10 * n * \log\left(\frac{d}{d_0}\right) + X_\sigma \qquad \text{eq. 4.2.1}$$

X_σ is a zero mean Gaussian distributed random variable with standard deviation σ. This term accounts for the fading effects that occur as a result of environment clutter, which produce varying path loss results between measurements of equal distance. A typical value for σ is 8dB for outdoor cellular system, and 5dB for an indoor environment [14]. Table 4.2.1 lists various path loss coefficients n for different environments [2].

Environment	Path Loss Exponent, *n*
Free Space	2
Urban area cellular	2.7 to 3.5
Shadowed urban cellular	3 to 5
Obstructed in building	4 to 6

Table 4.2.1 – Log Distance Path Loss Exponents

4.3. Hata Model

The Hata model is used to predict the path loss for cellular applications in urban environments where diffraction and multipath fading are common. Eq. 4.3.1 shows the standard equation for average path loss in an urban environment, where f_c is given in MHz. Transmitter – receiver separation d and transmitter height h_t are both given in meters. $a(h_r)$ is the correction factor for receiver antenna height and is shown in eq 4.3.2.

$$PL(urban) = 69.55 + 26.16\log(f_c) - 13.82\log(h_t) - a(h_r) + (44.0 - 6.55 * \log(h_t))\log(d) \quad \text{eq. 4.3.1}$$

$$a(h_r) = 3.2(\log(11.75 * h_r))^2 - 4.97 \quad \text{eq. 4.3.2}$$

The Hata model also provides modifications to eq. 4.3.1 in order to include suburban and rural areas, shown in eq. 4.3.3 and eq. 4.3.4.

$$PL(suburban) = PL(urban) - 2\left[log\left(\frac{f_c}{28}\right)\right]^2 - 5.4 \quad \text{eq. 4.3.3}$$

$$PL(rural) = PL(urban) - 4.78\,(\log(f_c))^2 + 18.33\log(f_c) - 40.96 \quad \text{eq. 4.3.4}$$

For these models, the antenna height correction factor $a(h_r)$ is also modified (eq. 4.3.5).

$$a(h_r) = (1.1 log f_c - 0.7)h_r - (1.56 log f_c - 0.8) \qquad \text{eq. 4.3.5}$$

This model is valid for the following constraints:

f_c : 150 MHz – 1500 MHz
h_r : 1 m – 10 m
h_t : 30 m – 200 m
d : 1 Km – 20 Km

During this testing, however, these constraints were not obeyed. 802.11b/g operates at 2.4 GHz, which exceeds the 1500 MHz limit of the Hata model. Also, this research assumes that transmitter height is at roughly ground level, which is far below the 30 meter minimum. Figure 4.3.1 was produced to compare recommended operational parameters against those used for this research. The graph shows urban, suburban, and rural environment path loss as a result of distance. The plots that adhere to the constraints use parameters h_t = 30m and f_c = 1500 MHz, while the plots that obey the parameters of this research use h_t = 1m and f_c = 2400 MHz.

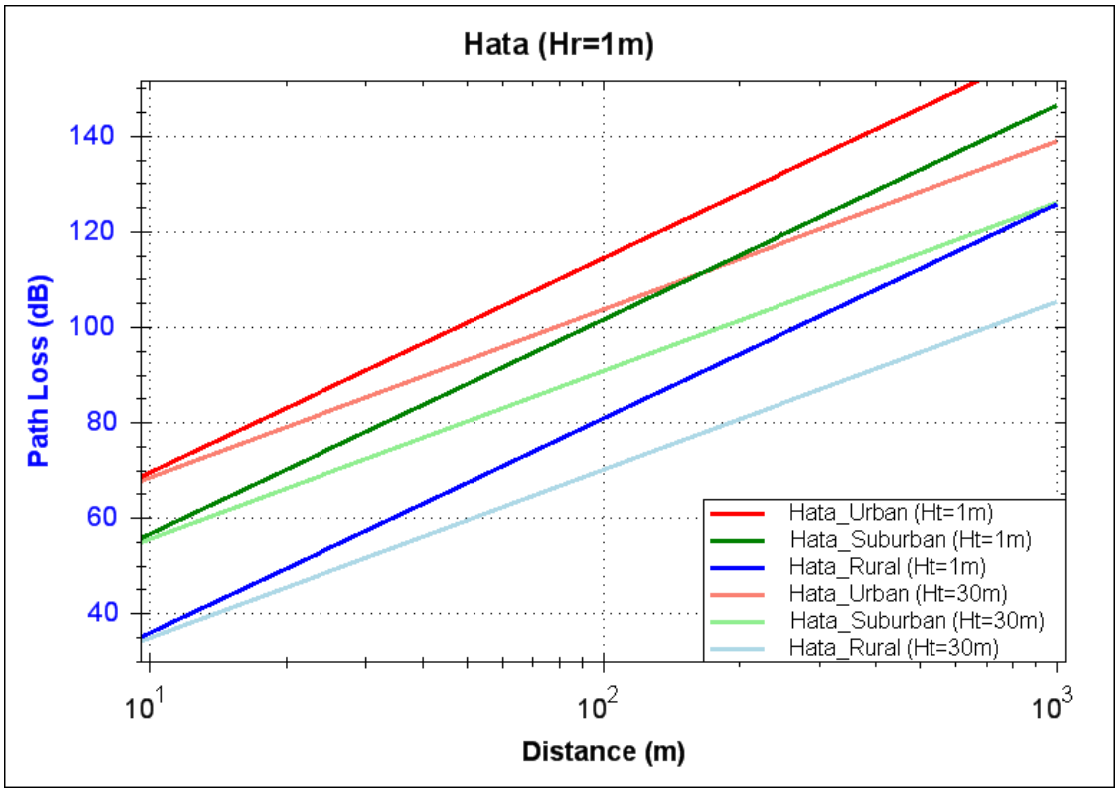

Figure 4.3.1 – Hata Path Loss

The results seem reasonable, as the only difference is a change in slope that results in higher path loss. For wireless systems, this behavior is expected as frequency is increased and transmitter height is decreased.

4.4. Cost 231 Model

The COST 231 model was developed as an extension to the Hata model in order to extend its frequency range to 1500 MHz to 2000 MHz, which is used in personal communication systems (PCS). The formula for this model is given in eq. 4.4.1, where the equation for receiver antenna height correction $a(h_r)$ from the Hata model is used. The environment correction factor C_M, is 0dB for suburban or rural areas and 3dB for

urban areas. The same constraints apply to this model as the Hata model, except for the change in frequency.

$$PL = 46.3 + 33.9\log(f_c) - 13.82\log(h_t) - a(h_r) + (44.9 - 6.55\log(h_t))\log(d) + C_M \qquad \text{eq. 4.4.1}$$

Although the frequency constraint for Cost 231 is relatively close to what is used by 802.11b/g, a large difference remains between recommended transmit height and the height used for this thesis. Figure 4.4.1 compares the two heights for urban and suburban settings, as the recommended parameters are h_t = 30 m and f_c = 2000 MHz, while the research specific parameters are h_t = 1 m and f_c = 2400 MHz.

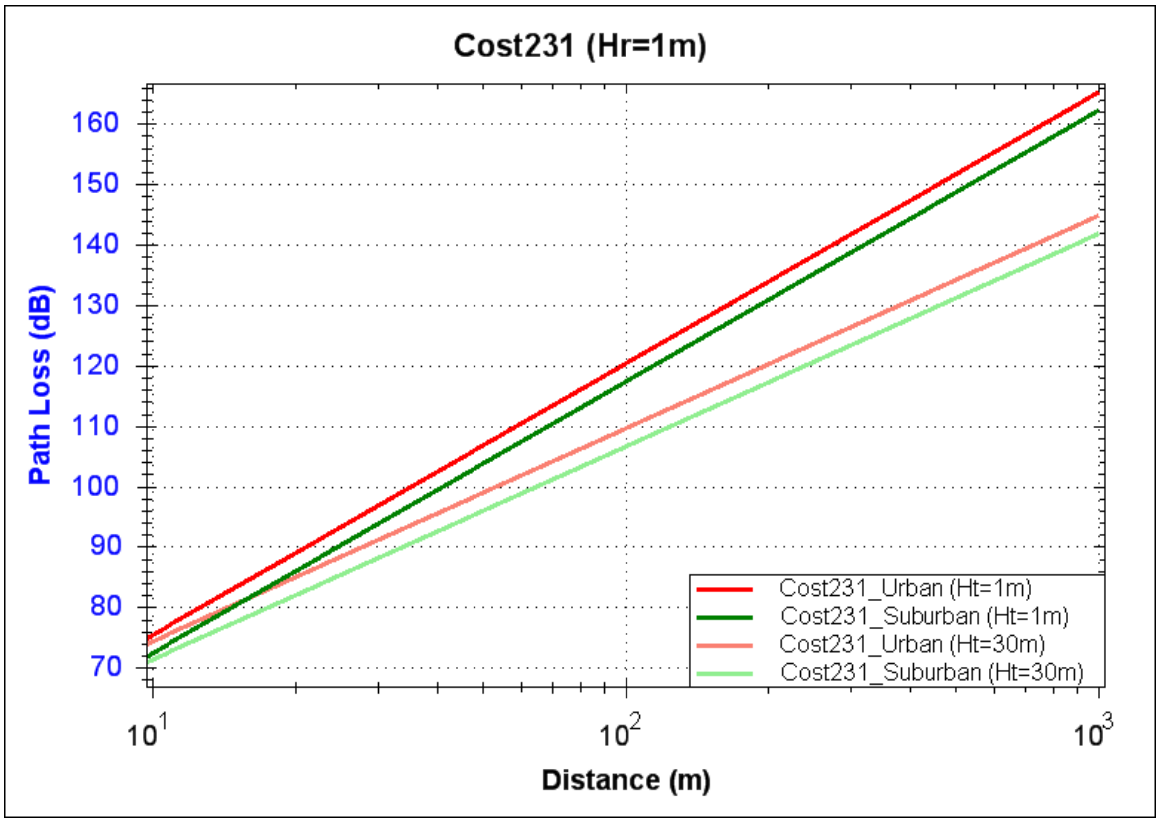

Figure 4.4.1 – Cost 231 Path Loss

Again, an increase in path loss is expected with a decrease in transmitter height. The plots otherwise seem reasonable enough to justify using the Cost 231 model for this research.

4.5 Stanford University Interim (SUI) Model

The SUI model was originally developed to address Multichannel Multipoint Distribution Service (MMDS) communication systems in the United States [4]. MMDS networks operate in the 2.5 GHz to 2.7 GHz frequency range, which makes SUI a good candidate for use with 802.11b/g. Three environments were accounted for in the SUI model, type A, B, and C [10]. Type A corresponds to maximum path loss as seen in urban environments or areas with heavy foliage or hills. Type B is more appropriate for suburban environments or areas with flatter terrain or light foliage. Type C is corresponds to minimum path loss and is appropriate for open environments with little to no propagation obstacles, such as rural areas. The equation for SUI path loss is given in eq. 4.5.1, where d is the transmitter-receiver separation in meters, d_0 is a 100 meter reference distance, and h_r is receive antenna height. The model specifies transmitter antenna height as 10m < h_b < 80m [4]. Coefficient ϒ is found by eq. 4.5.2, using the terrain specific values of a, b, and c from table 4.5.1. X_f and X_h are frequency and receiver antenna height correction factors, and are computed according to eq. 4.5.4 and eq. 4.5.5. The variable *s* is used to account for shadow fading and typically has a value of between 8.2dB and 10.6dB.

$$PL = A + 10 * \Upsilon * \log\left(\frac{d}{d_0}\right) + X_f + X_h + s \quad \text{, for } d > d_0 \qquad \text{eq. 4.5.1}$$

$$\Upsilon = a - bh_b + c/h_b \qquad \text{eq. 4.5.2}$$

Model Parameter	Terrain Type A	Terrain Type B	Terrain Type C
a	4.6	4.0	3.6
b	0.0075	0.0065	0.005
c	12.6	17.1	20

Table 4.5.1 – SUI Terrain Parameters

$$A = 20\log\left(\frac{4\pi d_0}{\lambda}\right) \qquad \text{eq. 4.5.3}$$

$$X_f = 6\log\left(\frac{f}{2000}\right) \qquad \text{eq. 4.5.4}$$

$$X_h = -10.8\log\left(\frac{h_r}{2}\right) \quad \text{, for terrain types A and B} \qquad \text{eq. 4.5.5}$$

$$= -20.0\log\left(\frac{h_r}{2}\right) \quad \text{, for terrain type C}$$

Although the frequency range for the SUI model is a close match for 802.11b/g, the model exhibits unexpected behavior when the transmit antenna height is below the recommended value. Figure 4.2 displays path loss for urban, suburban, and rural environments resulting from 1m and 30m transmit heights. The receive antenna was set at a height of 1m for both plots.

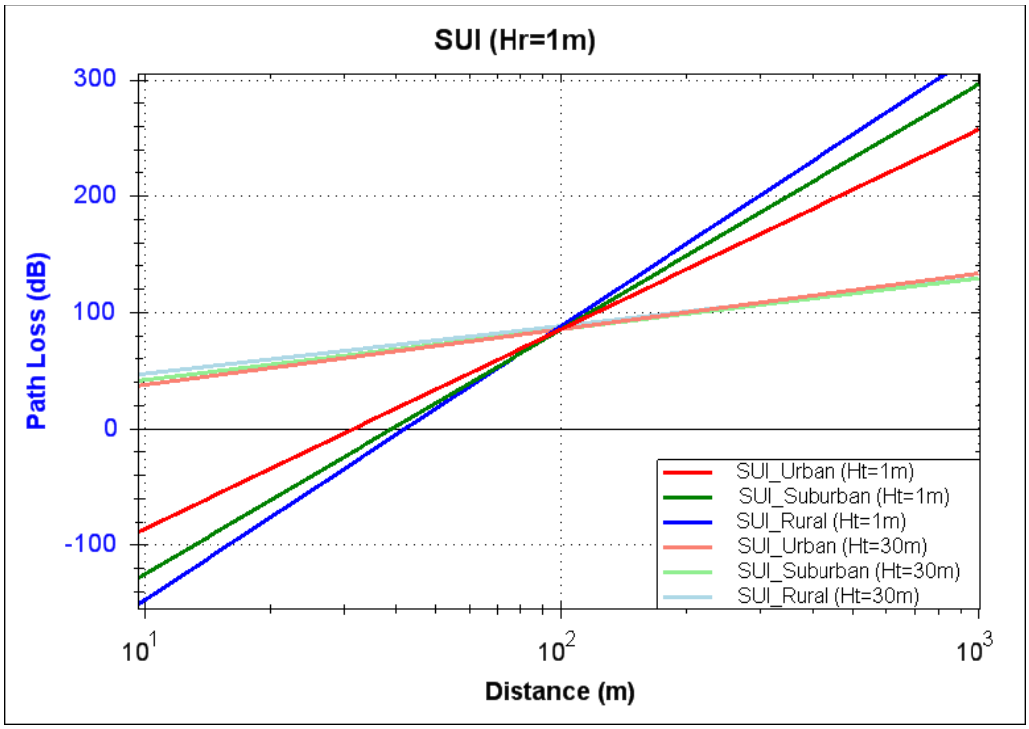

Figure 4.5.1 – SUI Path Loss

Notice that for the 1m transmit height curves, a gain is produced rather than a loss for distances less than 40m. Also, for distance greater than 100m, the graph shows that rural environment generates the greatest path loss, while urban environments produce the least loss. Due to these instabilities, the SUI model is unsuitable given the transmitter antenna height constraints of this research.

4.6. George Mason University (GMU) Indoor-Outdoor Model

The GMU model [19] was created on campus at George Mason University during the fall of 2007. It was produced in order to describe 802.11b/g path loss between an outdoor receiver and indoor transmitter, with each located at roughly ground level. The collection site consisted of a mixture of parking lots, multi-story brick buildings, and lawn areas

with light foliage. Suburban would be the best environment classification for the collection site. An AP was placed in an office with three or more cinder block walls separating it from the outdoors. The result was a modification to the COST 231 model (eq. 4.6.1), with the adjusted values highlighted in eq. 3.6.2. The GMU model was created using h_r = 1.7m and h_t = 0.7m.

$$PL(Cost231) = 46.3 + 33.9\log(f_c) - 13.82\log(h_t) - a(h_r) + (44.9 - 6.55\log(h_t))\log(d) + C_M \quad \text{eq. 4.6.1}$$

$$PL(GMU) = \mathbf{23} + 33.9\log(f_c) - 13.82\log(h_t) - a(h_r) + (\mathbf{22} - 6.55\log(h_t))\log(d) \quad \text{eq. 4.6.2}$$

CHAPTER 5

802.11 HARDWARE

The 802.11 hardware used for data collection during this research is discussed in this chapter. It consists of readily available, low cost devices that are typically found in commercial and residential networks.

5.1. AirPcap 802.11 Receiver

The Cace Technologies [24] AirPcap Ex wireless card was chosen as the 802.11 receiver. It has an MC card interface which allows an external antenna to be connected. Received signal strength indicator (RSSI) values are delivered in dBm format to a Windows user application. The drivers provide support for raw packet capture, as well as injection. The adapter contains an Atheros AR5523A baseband processor, and an AR5112 dual band radio [25], which provides support for 802.11a/b/g.

5.2. Linksys 802.11 Access Point

In order to provide values to use in baseline testing for range based propagation models, the transmit power and antenna gain was needed for a typical 802.11b/g transmitter. A Linksys WRT54G wireless router was chosen because of its widespread popularity and accessibility to its external antenna connectors. A Berkeley Varitronics Systems' Butterfly [20] handheld power meter was used to measure the transmit power, which was found to be 16dBm. As for the antenna, the WRT54G has dual omnidirectional elements that each has 2 dBi of gain [21].

5.3. 2.4 GHz Directional Antennas

Two directional antennas were chosen for the testing of AoA based methods. The first is Hyperlink Technologies' 2.4 GHz flat patch model HG2409P. It has a gain of 8dBi and horizontal and vertical half power beam width (HPBW) of 75° and 65°, respectively. The radiation pattern provided by the manufacturer [22] is shown in figure 5.3.1. The HG2409 is a relatively small antenna, measuring only 4.5 x 4.5 x .9 inches and weighing 0.4 pounds.

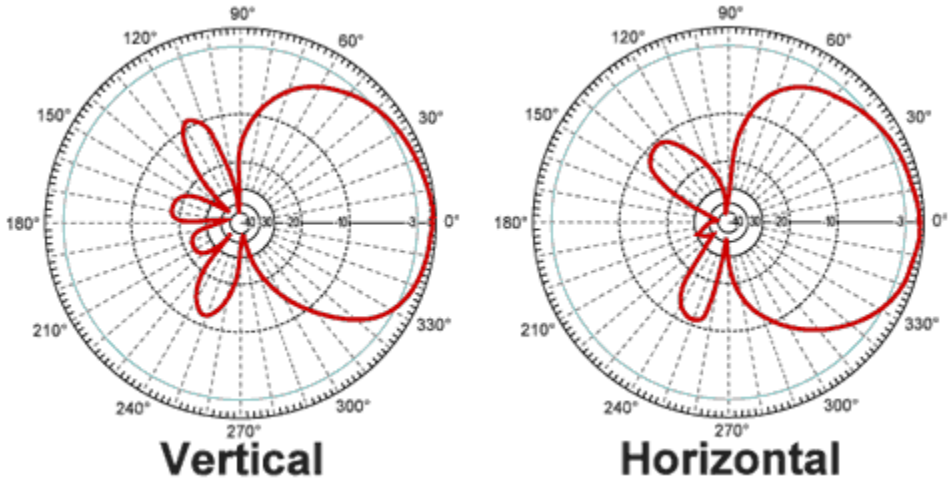

Figure 5.3.1 – HG2409P Radiation Pattern

The second antenna used in testing is the Hyperlink Technology HG2414P. It has higher gain than the HG2409, at 14dBi. The horizontal and vertical HPBW are both 30°, as shown in the manufacturer [23] provided radiation pattern in figure 5.3.2. It is roughly twice the size of the HG2409P, measuring only 8.5 x 8.5 x .1 inches and weighing 0.95 pounds.

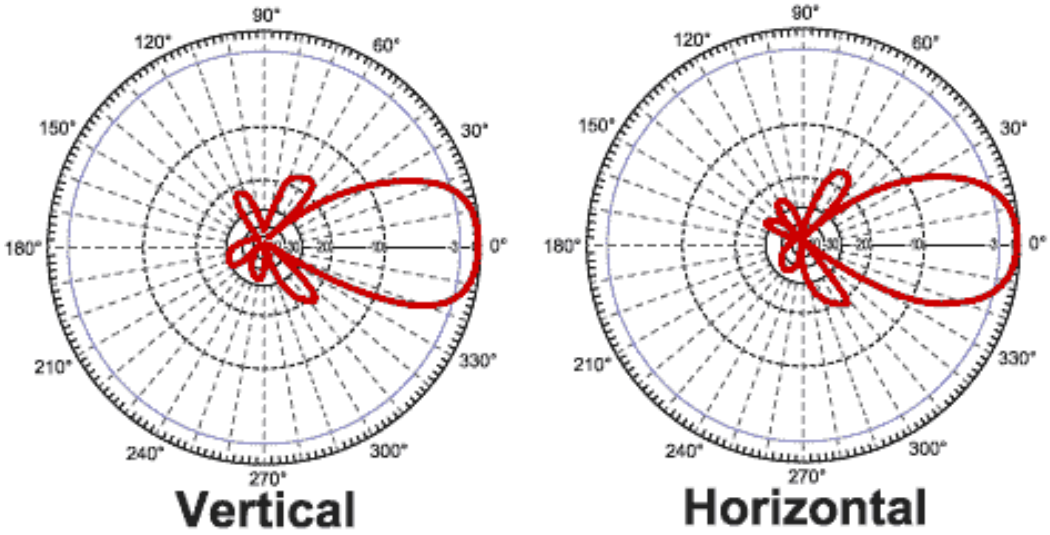

Figure 5.3.2 – HG2414P Radiation Pattern

5.4. 2.4 GHz Omnidirectional Antenna

Generally speaking, most omnidirectional antennas have very similar horizontal radiation patterns, which should have a nearly constant gain. The biggest difference between models is usually the overall antenna gain, which is inversely related to the vertical HPBW. For this research, it is assumed that source location is on roughly the same horizontal plane as the receiver, thus the vertical component can be ignored. For this reason only one antenna was used for omnidirectional testing, the Hyperlink Technology HG2407RD. It has a gain of 7dBi, and an adequately uniform horizontal radiation pattern, as shown in figure 5.4.1.

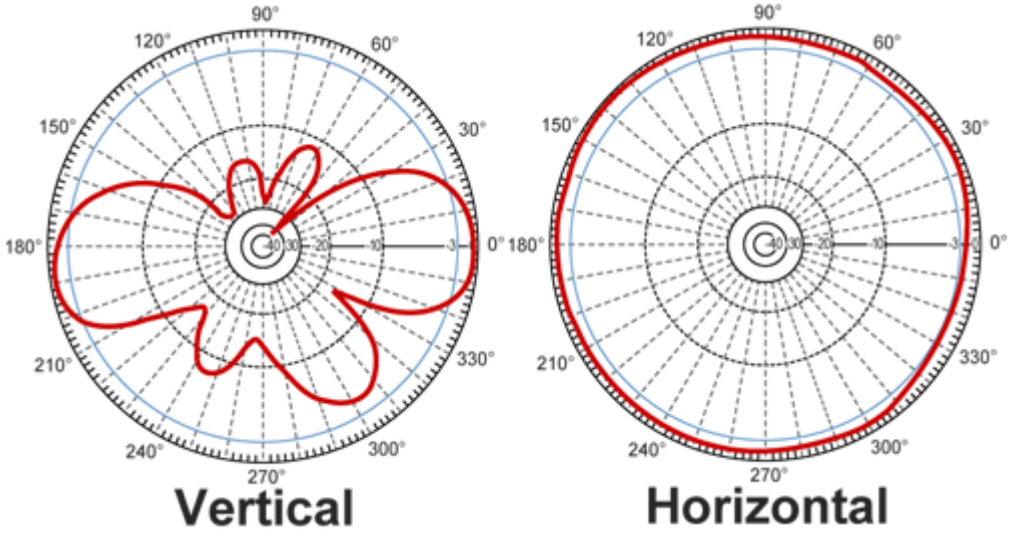

Figure 5.4.1 – HG2407RD Radiation Pattern

CHAPTER 6

COLLECTION ENVIRONMENT

6.1 The Links Apartment Complex

Data was collected in Stillwater, OK, and included three test sites. The first location was an apartment complex, shown in figure 6.1. The site consists of two story brick buildings and paved parking lots. There is no foliage on the site, however many stationary vehicles lined the space around the buildings. The AP was placed in a first floor apartment building, whose location is shown in figure 6.1 as the transmitter icon labeled "5545Test1." Collection points along with their corresponding distance from the transmitter are shown by the laptop icons. The upper left, upper right, and lower left locations are located 71.4 m, 47.2 m, and 58.7 m from the AP, respectively.

. Figure 6.1 – Links Test Site

6.2 Connell Street Apartment

The second test area included a split residential and commercial environment that contained a significant amount of foliage. The residential structures, on the left side of figure 6.2, were typically one story in height and constructed of brick. Two story commerical buildings lined with aluminum stand on the right side of figure . This suburban site was chosen for its foliage and mixture of building materials, which provides a wide range of propagation obstacles. The AP is shown in the center of the test site as the icon labeled “5545Test1”. The collection locations shown by the laptop icons are located 79.5 m (upper left), 82.1 m (upper right), 126.6 m (lower left), and 131.2 m (lower right) from the AP.

Figure 6.2 – Connell Street Test Site

6.3 Agriculture Hall Classroom Building

The third site, located on campus at Oklahoma State University, contained brick buildings, light foliage, and large open space parking lots. Two dormitory buildings, shown on the upper left hand side of figure 6.3, each stand 11 stories tall. The other structures shown are classroom buildings that range from 2 to 4 stories. This site was chosen because the large parking lots provide a more line of sight propagation path than the other two test areas. The known AP is labeled as "5545Test6," and was placed in a corner office. The collection locations are located 119.3 m (upper left), ,186.86 m (lower left), and 114.1 m (lower right) from the AP.

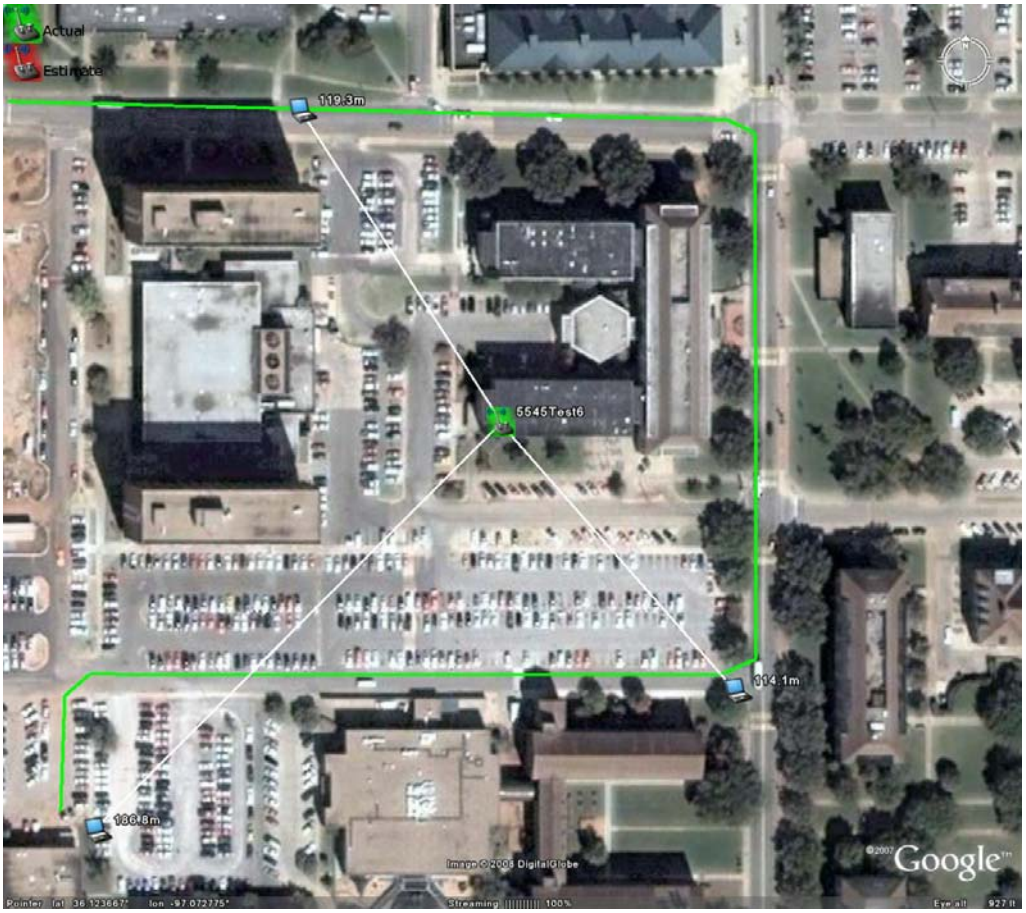

Figure 6.3 – Agriculture Hall Test Site

CHAPTER 7

DATA COLLECTION AND ANALYSIS

7.1. Access Point Setup

Localization of stationary access points (AP) is of primary concern for this research, thus an attempt to locate client nodes, which could potentially be mobile, is not made. Only beacons [15], which are capability description frames periodically transmitted by an AP, were collected in order to ensure that only APs were targeted. It is important to note that passive collections are possible because beacon frames are sent without client request by default. For this research, beacon frames were sent at 10 Hz using transmit power as described in section 5.2. Once a beacon frame is received, the source MAC address, SSID, and RSSI are all stored in a database. In order to accurately establish measurement location, latitude and longitude readings were also stored. Collectively, this data is used in order to estimate the AP location and for visualization using Google Earth.

Prior to data collection, an AP was placed in an indoor environment, with approximately 20-25 feet of separation between the transmitter and window. This separation is important in order to ensure a realistic test case, as a transmitted signal close to a window does not experience typical indoor propagation obstacles and can yield uncharacteristically accurate estimation results.

7.2. Stationary Omnidirectional Collection

This method consisted of a single HG2407RD omnidirectional antenna which was magnet mounted perpendicularly to the roof of a compact car. Random locations within range of the AP were chosen and data was collected for roughly 30 seconds at each point. Figure 7.2.1 shows the application used to collect, store, and analyze test data.

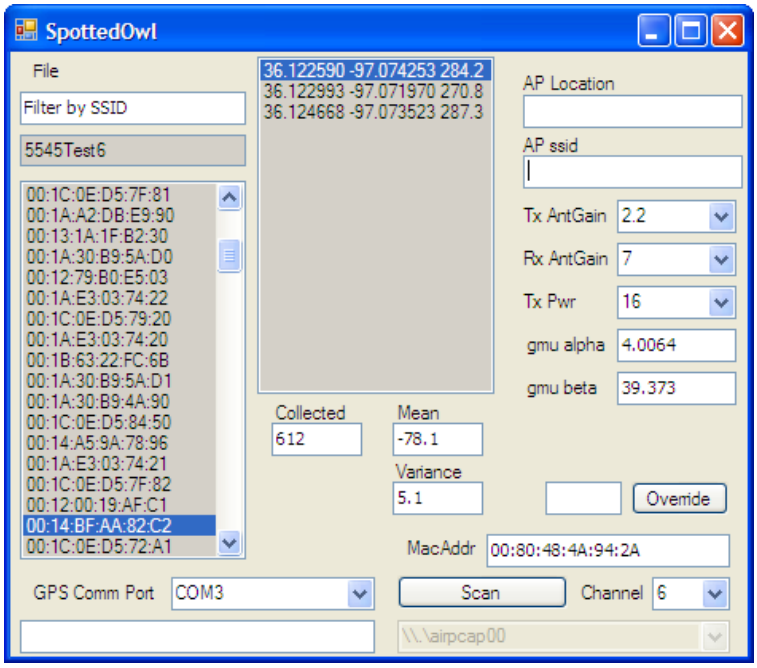

Figure 7.2.1 – SpottedOwl Omnidirectional Application

Once three or more points are collected, a specific location can be estimated using the propagation model equations described in chapter 4. The mean and variance is found for all values collected at each stationary point. Figure 7.2.2 shows a typical distribution of RSSI values for a 30 second stationary collection. Since the RSSI value reported by the AirPcap is in units of dBm, these values can be plugged directly into a propagation model in order to find a range.

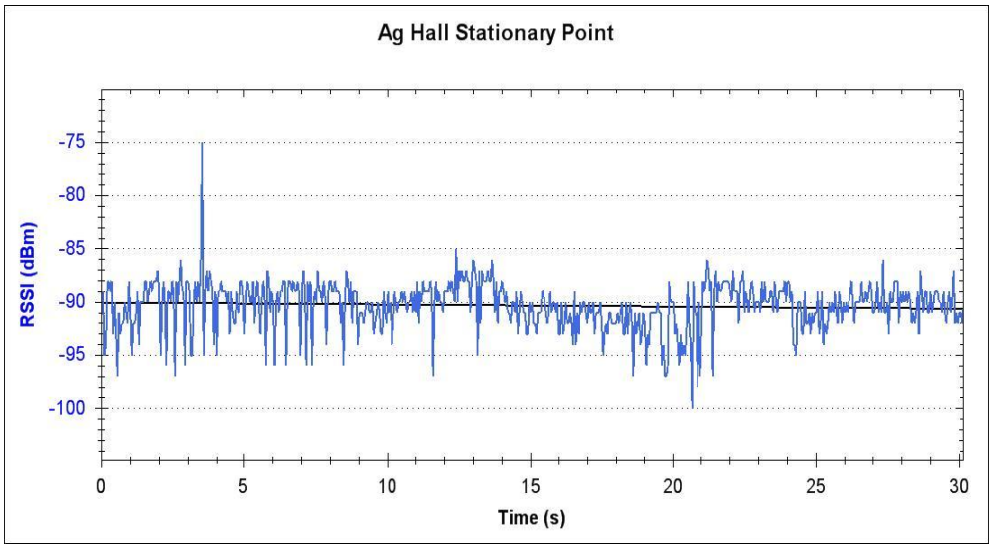

Figure 7.2.2 –Stationary Signal Strength Distribution

Several different propagations models were evaluated in order to determine best overall performance, including Free Space, GMU, Hata, and Cost 231. Path losses for these models were computed using a transmitter and receiver height of 1 meter and frequency of 2400 MHz. The path loss curves for each of these models are compared in figure 7.2.3.

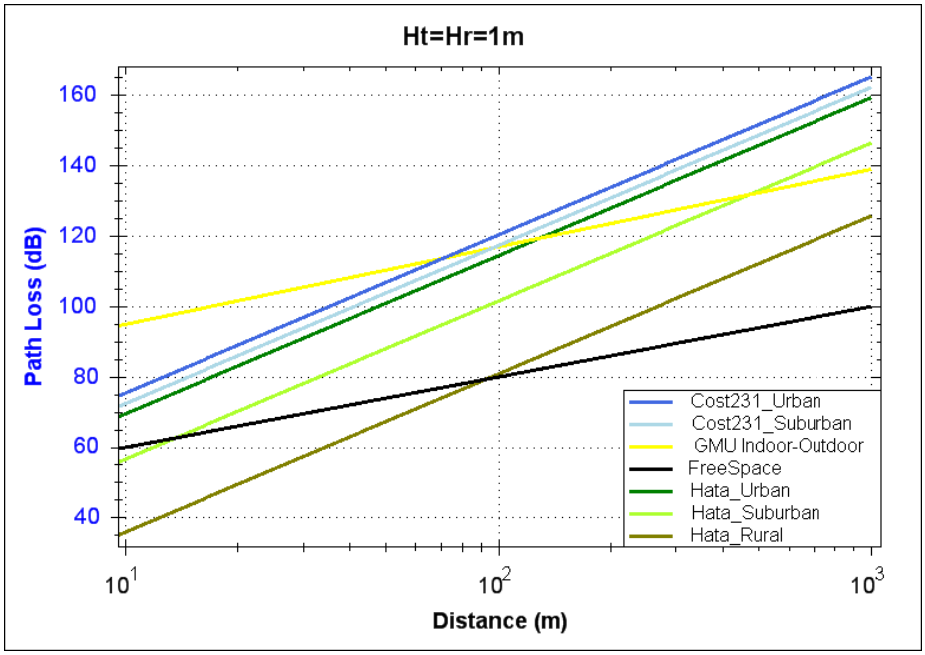

Figure 7.2.3 – Propagation Model Path Loss Comparison

After range estimates for each stationary point have been computed, a least squares intersection is found using multilateration as described in section 3.2. Intersection and range estimates are visualized using Google Earth, shown in figure 7.2.4. The red circles show the range estimated by a particular model, and the laptop icons indicate the collection point and average RSSI value. A green transmitter icon designates the actual AP placement, while the red icon identifies the estimate location and model used. The accuracy of this method for each specific test site will be shown in section 8.1

.

Figure 7.2.4 –Stationary Onmidirectional Visualization

7.3. Mobile Omnidirectional Collection

Identical hardware was used for this technique as in the stationary omnidirectional method. However, rather than collecting from several stationary points for extended periods of time, data was captured as the vehicle was in motion on the test site. Each signal strength measurement was stored corresponding to the location at which it was received, and multiple readings for a single point were averaged.

Analysis for this technique includes range estimation using the same propagation models mentioned in section 7.2, and multilateration is also used to estimate the source location. The computational complexity is increased with respect to the stationary case due to the potentially large number of data points. However, this can be conveniently overlooked because analysis is performed post collection rather than in real time. Figure 7.3.1 shows an example of predicted range and location estimates along a drive path.

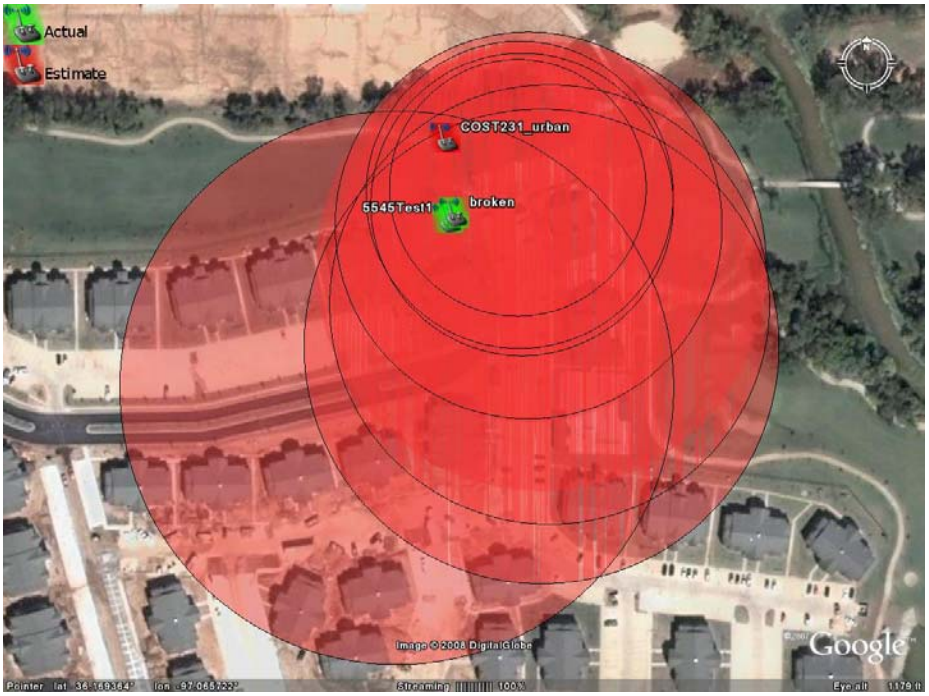

Figure 7.3.1 –Mobile Range Based Visualization

7.4. Stationary Directional Scanning Collection

For this method, a single directional antenna mechanically rotates around the azimuth plane at 0.75 revolutions per minute. The antenna is mounted atop an aluminum cylinder housing that is covered by an acrylic overlay. The contents of this housing, shown in figure 7.4.1, include an AirPcap 802.11 receiver, motor, motor controller, and a GPS sensor. An electronic compass is used to establish azimuth orientation. However, the sensitivity of the compass to external magnetic fields requires special care to be taken when mounting the device. This is done by elevating the compass 1.5 feet above the vehicle body, antenna, and electronics using acrylic rods. Also, rubber suction cups are used to secure the collection device to the vehicle roof rather than a magnet, which ensures that no unnecessary ferrous metals are present in the local environment.

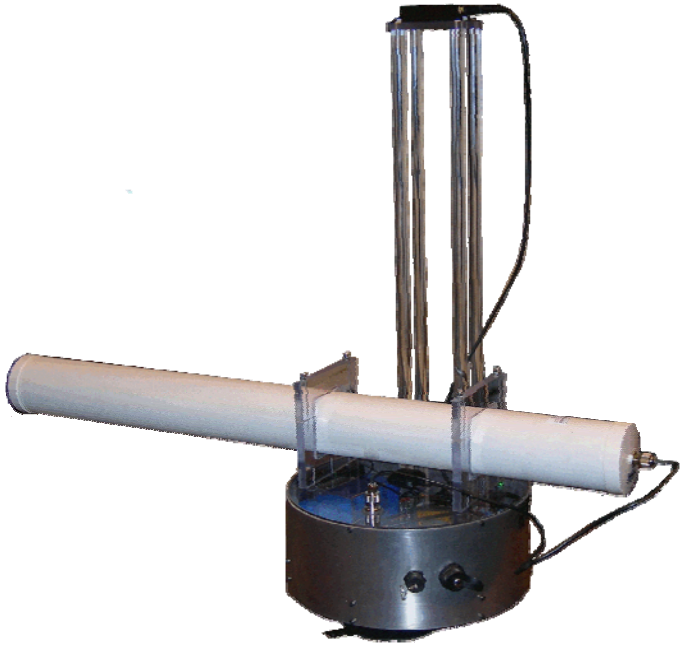

Figure 7.4.1 – Mechanically Scanned Collection Tool

Data is collected in a stationary manner by stopping the vehicle and making a 360º scan of the environment. The RSSI value for each incoming packet is stored in a database along with the location and corresponding azimuth at the time of reception. Scans are performed at multiple locations for a given area in order to obtain several AoA measurements. Identical tests were performed using two directional antennas, the HG2409P and HG2414P.

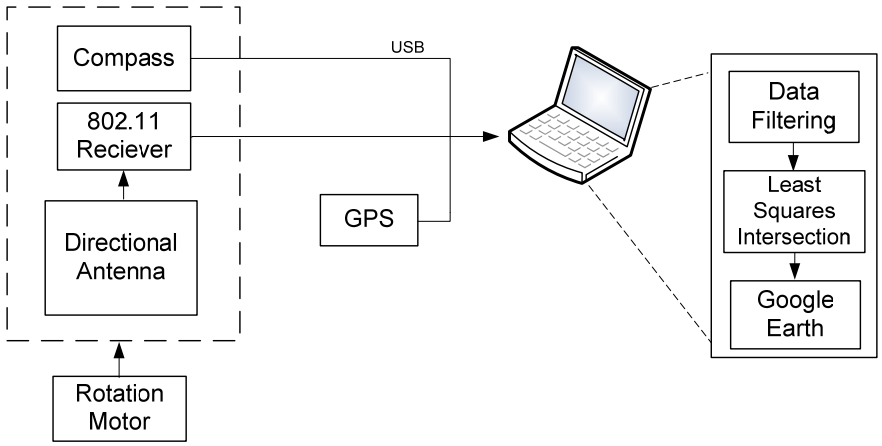

Figure 7.4.2 – Scanning Directional Diagram

After multiple scans for a given site have been completed, the data is analyzed in order to make a source location prediction. The first step is to filter the raw data for each scan point, which requires averaging and smoothing functions. Figure 7.4.3 shows the raw data overlaid onto its corresponding geographic location. Notice that multiple vectors are often overlapping each other. This is a result of multiple RSSI values being associated with a single integer azimuth. When this is the case, the average is computed in order to produce a single signal strength value. A median filter is performed across the entire scan to remove outliers, which could produce a false angle of arrival measurement. This is followed by linear regression filtering used to smooth over the entire scan. Figure 7.4.4

shows the difference between the raw scan data and the resulting filtered scan data. Note that for all geographic plots such as these, the top of the figure is north, and 0º, 90º, 180º, and 270º represent north, east, south, and west, respectively.

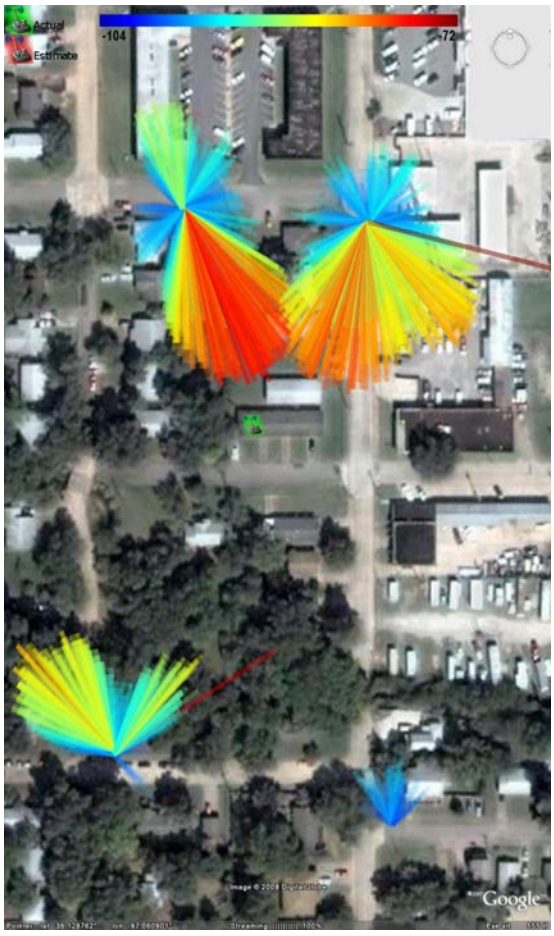

Figure 7.4.3 – Raw Scan Data

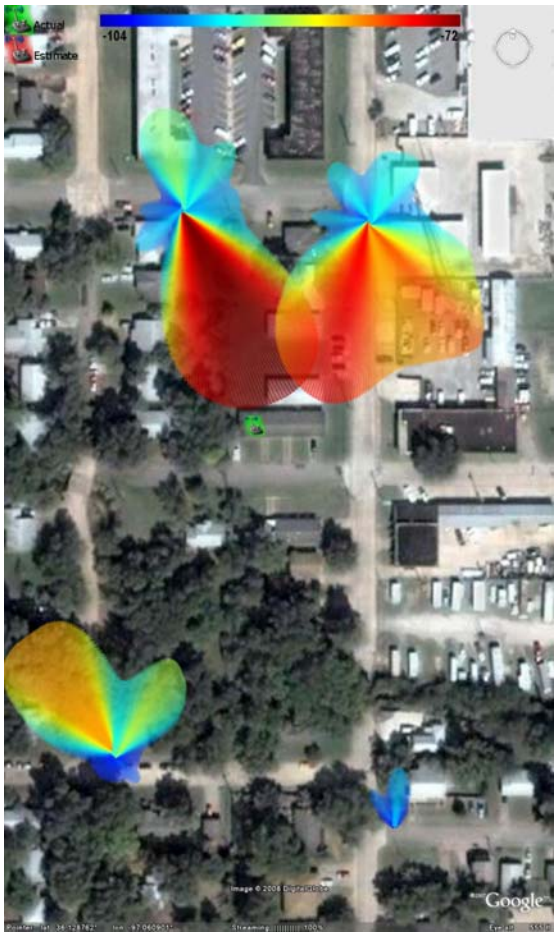

Figure 7.4.4 – Filtered Scan Data

Figures 7.4.5 show the difference between the raw and smoothed data for a single scan point. However, this plot also shows the gain with respect to geographic direction, where each green line represents 3db of attenuation.

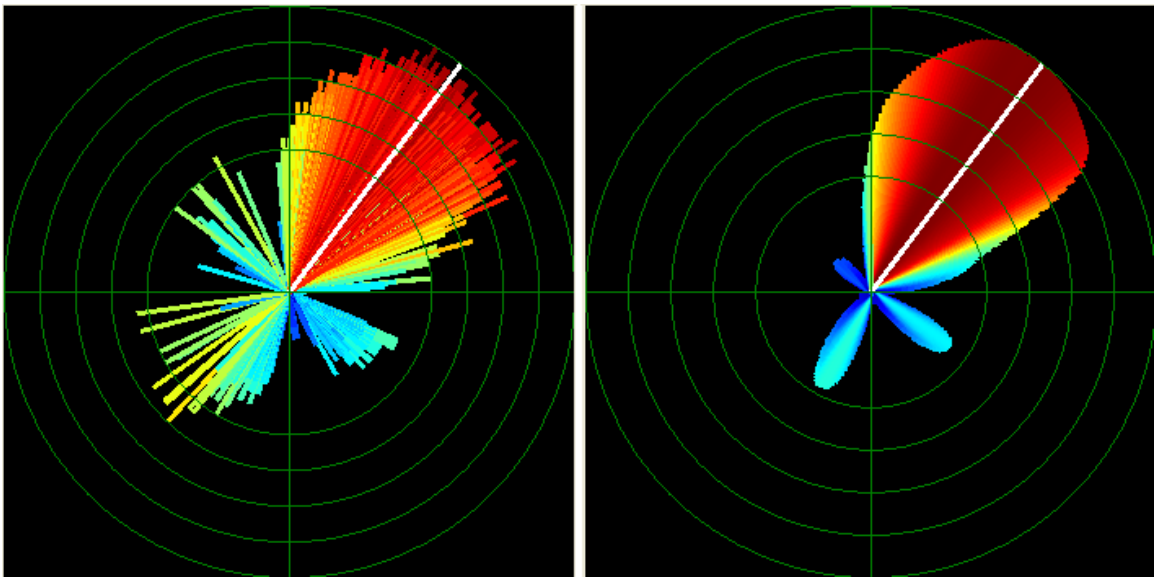

Figure 7.4.5 – Single Point Filtered Scan Data

In order to identify collections in which multipath is present, a comparison is made between the antenna beam pattern in the presence of no multipath and the beam pattern of the actual collected data. However, because the collection device was mounted atop an automobile and included various fixed reflecting structures; a beam pattern was needed that took into account the factors specific to this collection device. The best option for this is an anechoic chamber, but one large enough to accommodate a vehicle was not available. The next best option was to find a large, flat, open area in which a full 360º scan could be obtained. A rural site was found that offered unobstructed terrain of over a mile in diameter. A battery powered AP was placed 1m above a dirt road; its location shown by the green icon in figures 7.4.6 and 7.4.7. With the front of the vehicle facing 180º (south), a full rotation was made with each antenna. The resulting radiation pattern for the HG2409P and HG2414P at this site is shown in figures 7.4.6 and 7.4.7.

The very low resolution terrain data for this site is a result of the remote location. These controlled tests provided the baseline antenna radiation patterns used for analysis.

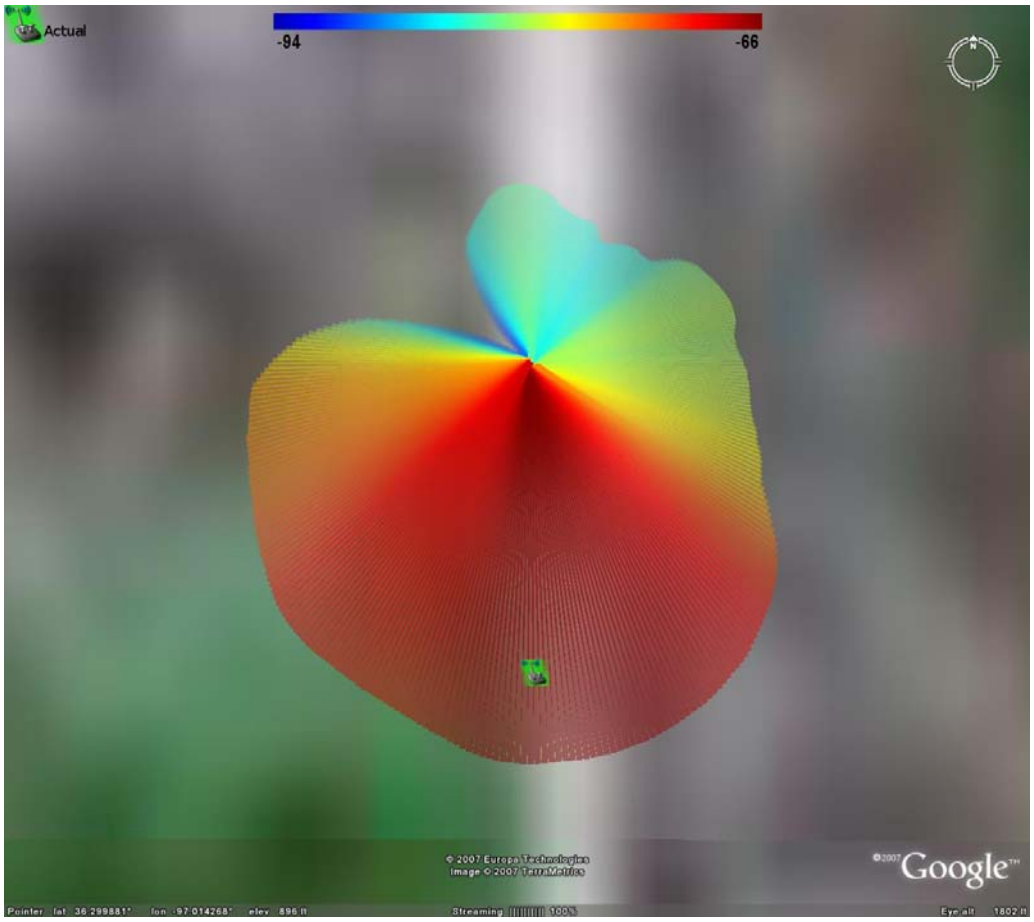

Figure 7.4.6 – HG2409P Baseline Scan Pattern

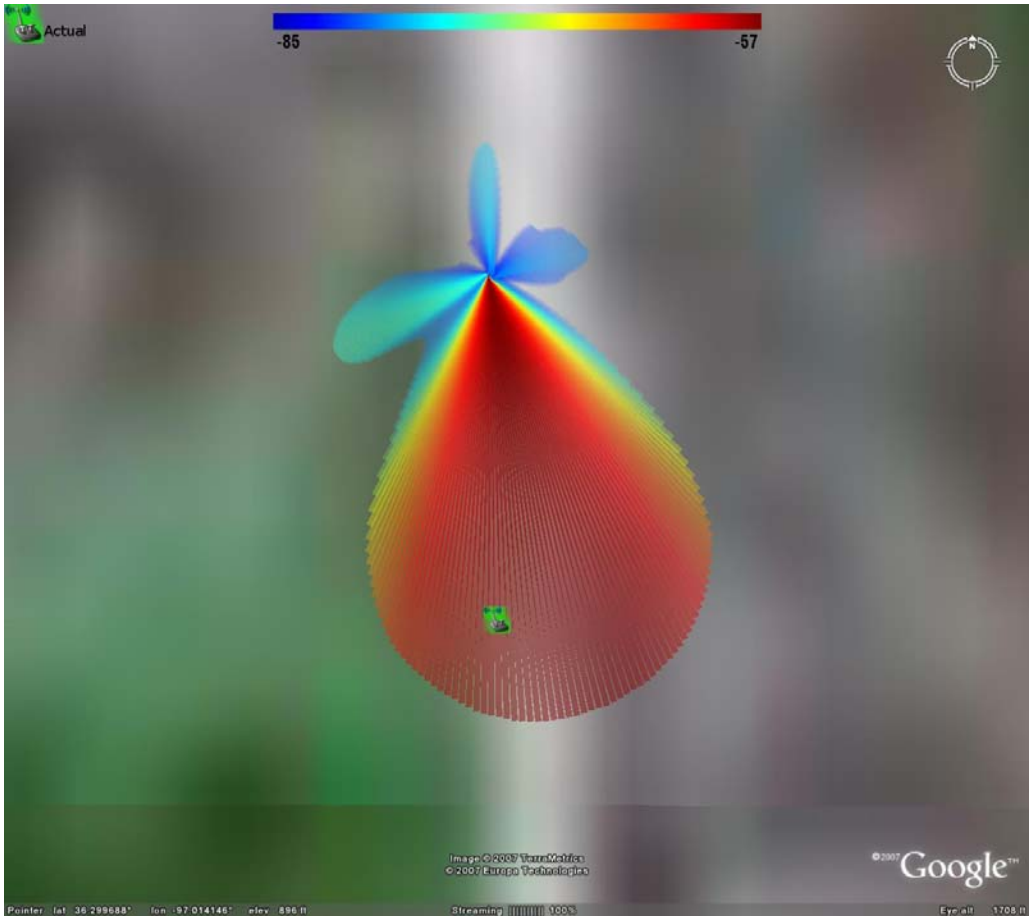

Figure 7.4.7 – HG2414P Baseline Scan Pattern

The filtered data for each point is compared to the baseline antenna scan by aligning the highest signal strength for both. This is done in the analysis program by rotating the baseline scan until its mainlobe peak matches up with the peak of the test data. Figure 7.4.8 shows the comparison between the baseline and test scan patterns, as the blue and green lines, respectively. After both patterns are aligned, the correlation coefficient [18] between them is calculated using eq. 7.4.1.

$$\rho = \frac{cov(x,y)}{(\sigma x * \sigma y)} \qquad \text{eq. 7.4.1}$$

This value is multiplied by the average signal strength value for the test scan in order to calculate a score for the test point. The average value is used under the assumption that the location that receives the most signal has the best "view" of the transmitter. Scores are used to rank each point for an entire site, and are also used as weights when calculating a location estimate using weighted least squares.

In an environment which multipath is significant, it is difficult to distinguish reflected signals from the true AoA from the transmitter. The possibility exists that the main peak corresponds to multipath, in which case another peak could exist in the radiation pattern corresponding to transmitter location. Therefore, the entire scan must be inspected to determine if signal peaks exist outside the bounds defined by the baseline pattern. This is done by simply by subtracting the baseline from the test scan pattern, shown by the red line in figure 7.4.8. Linear regression is used to smooth these values, shown by the orange line. This smoothed data results in a single peak value that exists outside the baseline antenna pattern. The grey bars show the peak values that are designated as potential AoA values, and correspond to the green lines in figure 7.4.9. At this point in the analysis, it is not known whether the peak values are the true AoA or multipath. This is determined later by an iterative peak comparison between points.

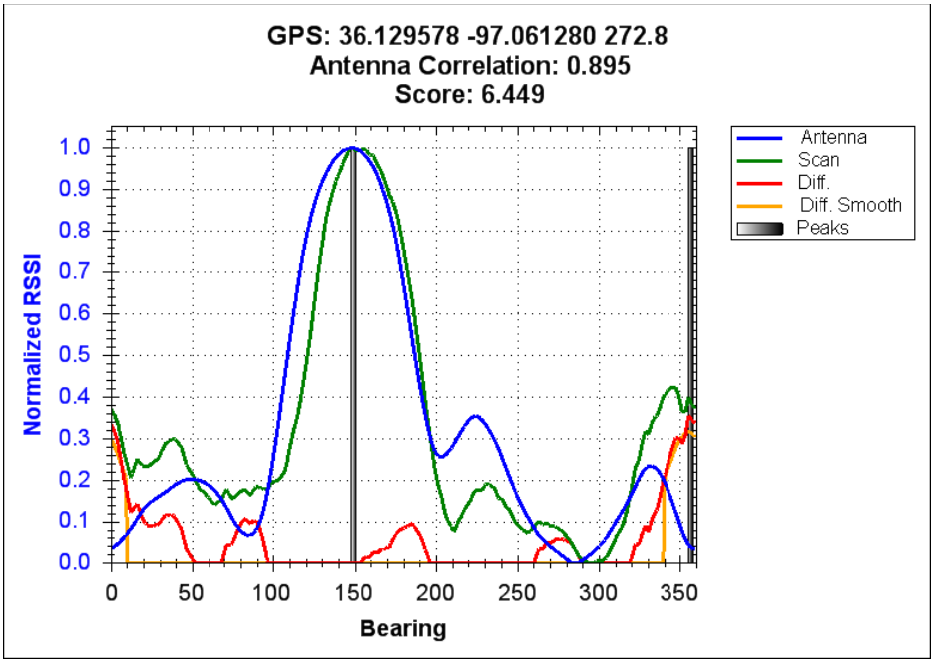

Figure 7.4.8 – Baseline, Test Pattern Comparison

The scan with the highest score is chosen as the reference value by which peaks values for all other points are compared. This is done on a point by point basis according to each point's score. For instance, figure 7.4.9 shows the beam pattern and peak values for the highest scoring scan for the entire test. Therefore, it is the reference by which all other values are compared.

Figure 7.4.9 – Reference Scan for Test Site

The second highest scoring point is compared with the reference point in figure 7.4.10. The peaks for this location that intersect with the peaks for the reference location are kept, while those that do not intersect are removed from the data set. The remaining peak values are shown in figure 7.4.11, with the non-intersecting vectors removed.

Figure 7.4.10 –First Scan Comparison

Figure 7.4.11 –Result of First Scan Comparison

The third ranked scoring point is added in figure 7.4.12 and is compared with the reference point peaks. Of the two peak vectors for this point, only one intersects with a reference point vector. In this case, the multipath present at this point was stronger than the true AoA signal. By iteratively comparing with the intersections of other peak vectors, the AoA vector that resulted from multipath was identified and eliminated. It is not visible on the map in figure 7.4.12, but there are houses within the foliage that correspond to the direction of the multipath.

Figure 7.4.12 –Second Scan Comparison

The intersection with the second and third ranked peak vectors validate the correct AoA vector for the reference point, which points southeast. Therefore, the other reference peak is removed from the data set, as well as all other vectors associated with it. The result of this is shown in figure 7.4.13.

Figure 7.4.13 –Result of Second Scan Comparison

The final, lowest ranked point is then compared with the remaining reference vector in figure 7.4.14. Only one of the two peak vectors for this point cross the reference, and thus the other is eliminated from the data set.

Figure 7.4.14 – Third Scan Comparison

The estimate location for this test site is indicated by the red transmitter icon in figure 7.4.15. This is the result of a weighted least squares intersection calculation, using the scores for each location as the weights. Notice that the peak vector for the scan location in the southeast corner of the figure is not indicative of the true transmitter location. However, the overall estimate is not greatly affected due to that particular location having a much lower score relative to the other points.

Figure 7.4.15 –Result of Third Scan Comparison

Notice that for this test site, the estimated location icon has the number 22.7 beside it. This corresponds to the sum of the differences between true angle to estimate, shown by the dashed white lines in figure 7.4.16, and the measured peak vectors, shown by the green lines. This value is essentially a measure of interior area of all AoA vectors used for the weighted least squares calculation. In the case that more than one estimate is made for a given site, multiple icons and angle difference values will be shown, with the lowest value corresponding most accurate estimate.

Figure 7.4.16 – Angle Differences

Figure 7.4.17 shows the application used to receive, store and analyze data for this collection method. The plot on the bottom left shows the unfiltered signal strength vs. bearing, while the top and bottom right graphs display the smoothed data. The green circles on the polar plots show the 3dB attenuation points.

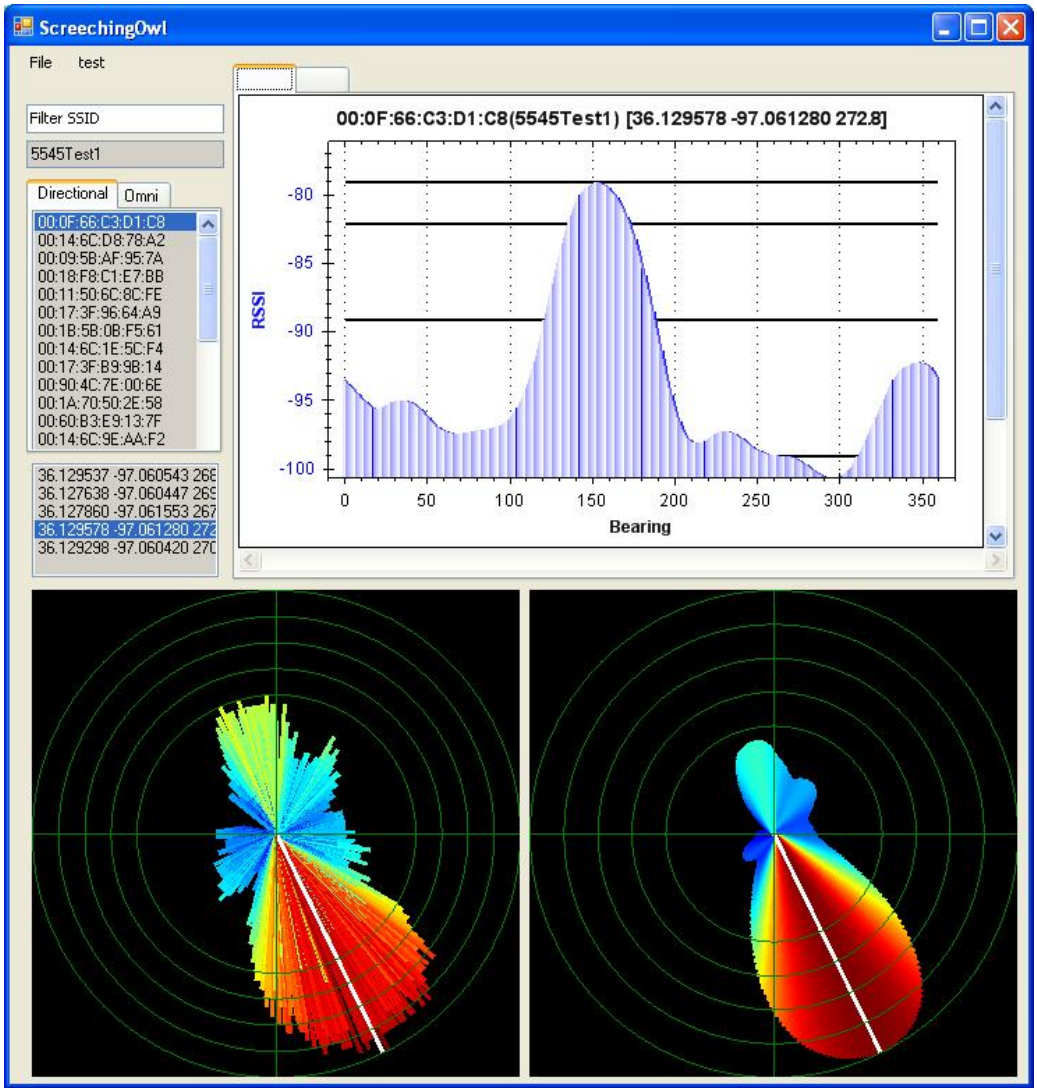

Figure 7.4.17 – ScreechingOwl Application

7.5. Mobile Directional Array Collection

This method consists of a directional antenna array that is magnet mounted onto the top of a vehicle. Data is collected while the vehicle in motion, and the location and heading are determined by the GPS sensor. The array consists of four directional antennas that are spaced 90º apart. An array of HG2409P 8dBi antennas (shown in figure 7.5.1), as well as HG2414P 14dBi antennas (shown in figure 7.5.2) were both tested using this method. The estimated overall radiation pattern for each of these arrays is shown in figures 7.5.3 and 7.5.4, corresponding to the HG2409P and HG2414P arrays, respectively. The dark green lines in these figures each represent 3dB of signal attenuation.

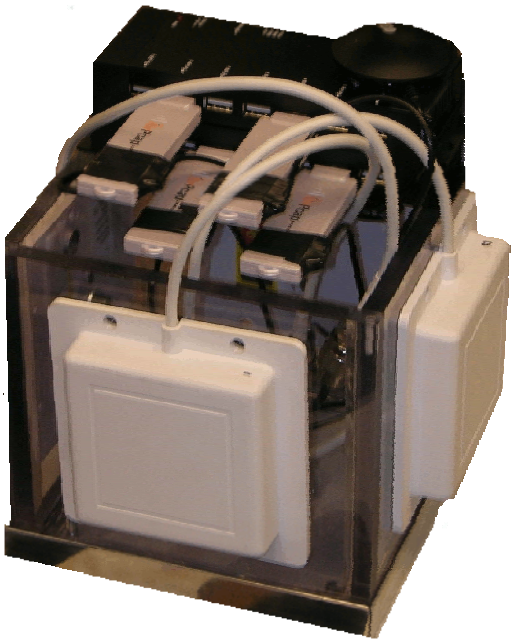

Figure 7.5.1 – HG2409P Array

Figure 7.5.2 – HG2414P Array

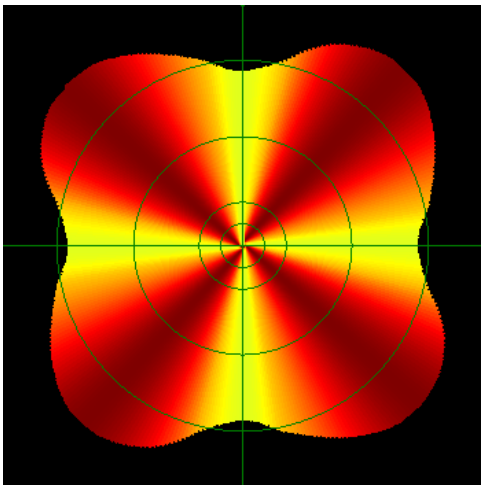

Figure 7.5.3 – HG2409P Array Pattern

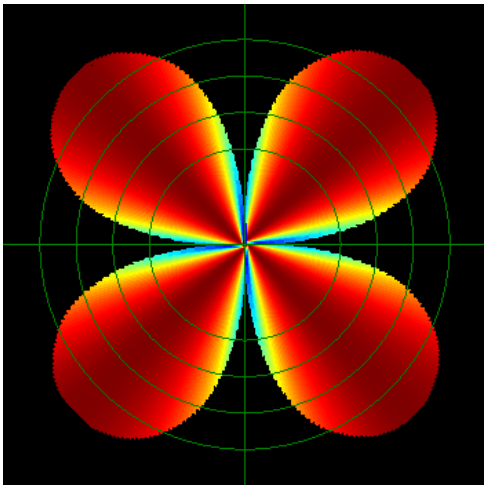

Figure 7.5.4 – HG2414P Array Pattern

Each antenna has its own dedicated 802.11 receiver, which enables all traffic to be captured and stored according to that particular antenna's geographic heading. Figure 7.5.6 depicts how the antenna array is situated atop the vehicle, with the edge between antenna elements 0 and 3 always facing the front of the car. Again, note that 0º, 90º, 180º, and 270º represent north, east, south, and west, respectively. For instance, in figure 7.5.6, the vehicle is travelling due North (0º). In this configuration, signals received at antenna elements 0, 1, 2, and 3 are stored using AoA of 45º, 135º, 225º, and 315º, respectively. Figure 7.5.7 shows the vehicle travelling Northeast (45º), which results in all arrival angles being shifted +45 º. For any vehicle heading N, arrival angles are shifted as follows:

Antenna 0: N + 45º
Antenna 1: N + 135º
Antenna 2: N + 225º
Antenna 3: N + 315º

If the shifted antenna angle result is > 360º, then an angular wrap around function repositions it between 0º - 360º.

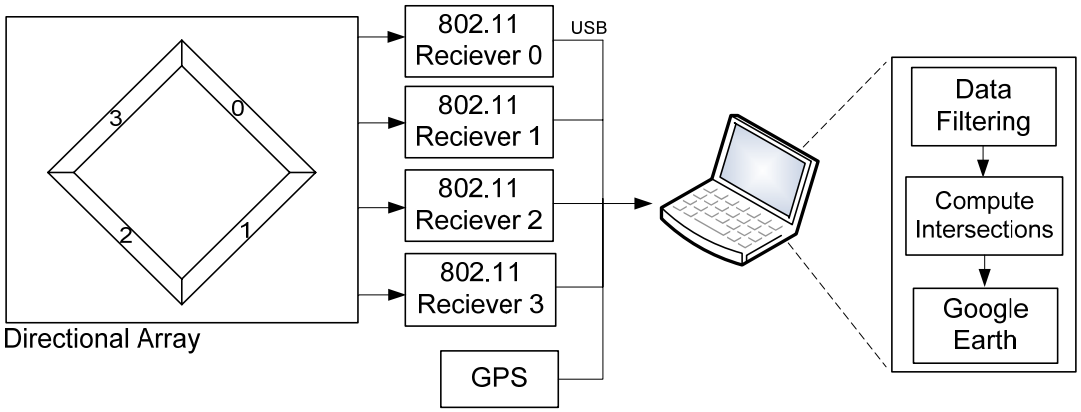

Figure 7.5.5 –Mobile Directional Array Collection Diagram

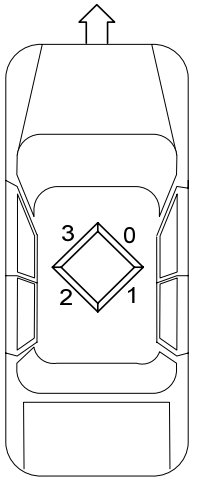

Figure 7.5.6 –Array Facing North

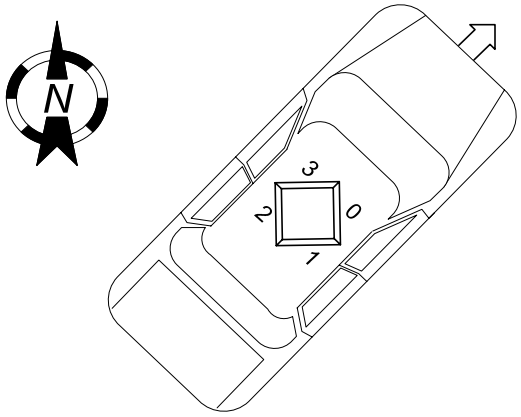

Figure 7.5.7 –Array Facing Northeast

The antenna elements are arranged in this manner in order to obtain an intersection of lines when traveling in a straight path, as shown in figure 7.5.8. If the array was not rotated 45º with respect to the forward motion of the vehicle, this intersection would not take place.

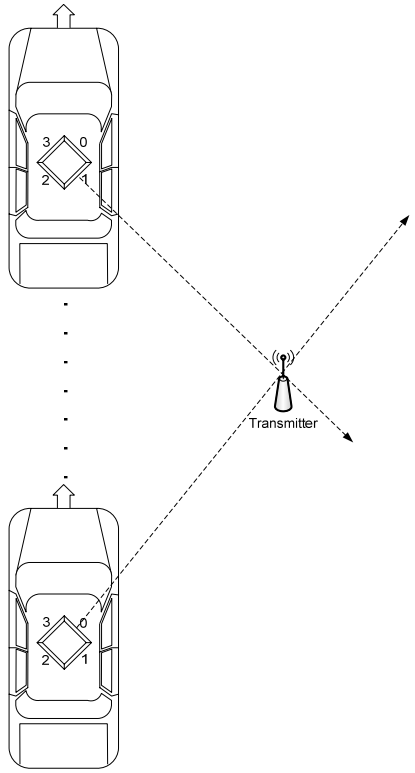

Figure 7.5.8 – Array Linear Path Intersection

After data for a particular site has been collected, multiple vectors for each GPS point exist, as shown in figure 7.5.9. In order to obtain a source location estimate, this data must be combined and filtered for analysis. First, the measurements for each GPS point are summed using vector addition. Because the RSSI values returned from the AirPcap adapter are logarithmic (dBm), each vector must be converted to a linear scale before addition takes place. It is converted back to logarithmic scale after addition. The result is shown in figure 7.5.10.

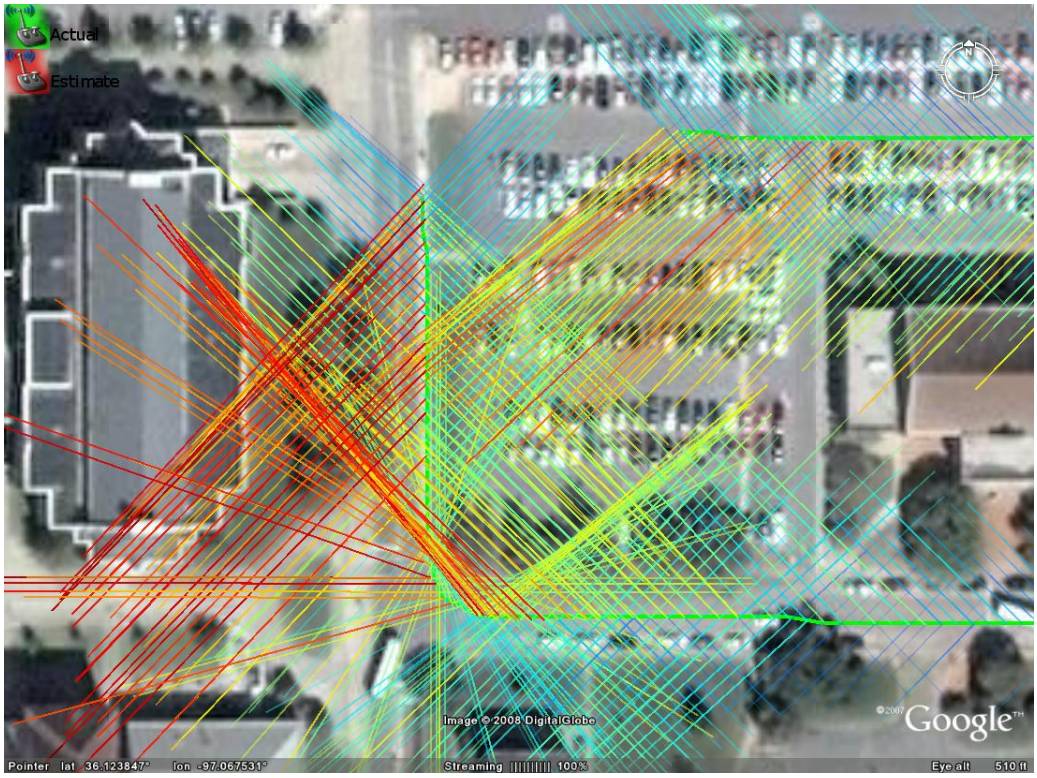

Figure 7.5.9 – Raw Array Data

Figure 7.5.10 – Vector Added Array Data

After the resultant vectors are found, a median filter is applied to the vector headings in order to remove directional outliers, as shown in figure 7.5.11. This is particularly beneficial in removing data collected while the vehicle is making turns, which often yields false arrival angles due to slow GPS update rate.

Figure 7.5.11 – Median Filtered Array Data

Next, the variance of each bearing with respect to that of its neighbors' is calculated. If the result is above a certain threshold, that vector is removed from the data set. This ensures that only consistent AoA measurements remain in the data set prior to predicting a source location. The result of this filter is shown in figure 7.5.12.

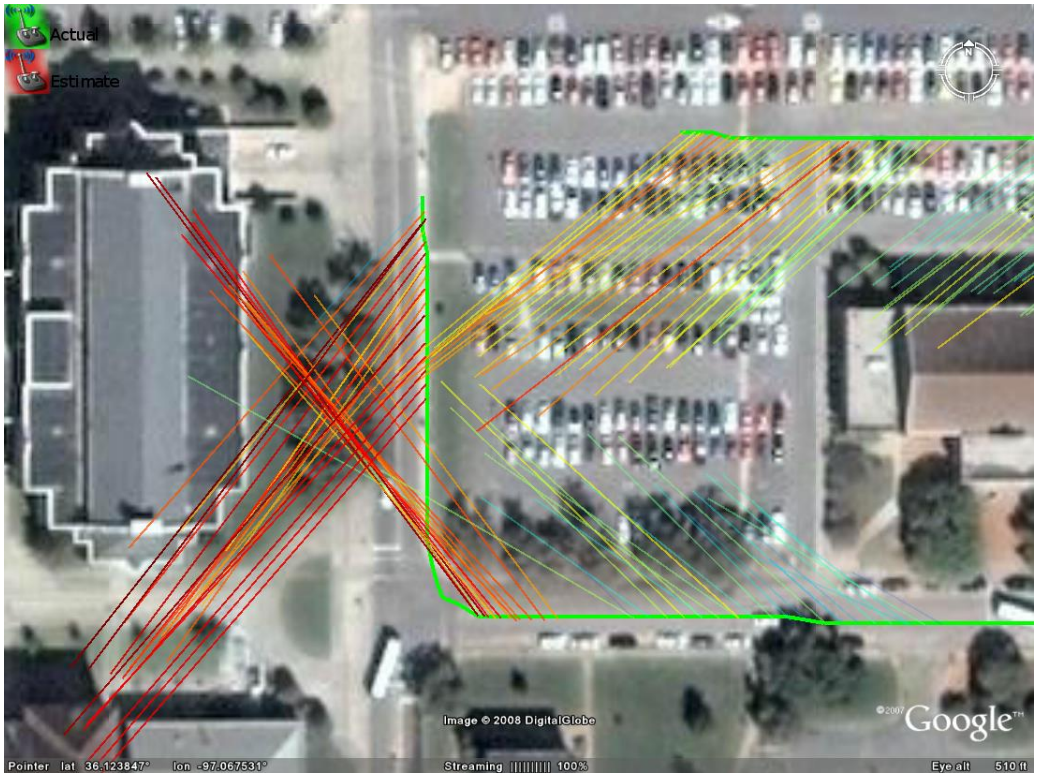

Figure 7.5.12 – Variance Filtered Array Data

Finally, the intersection of all remaining vectors is calculated along with the result of their signal strengths. The source location estimate is chosen by the intersection that has the highest resultant signal strength. All possible intersections are shown in figure 7.5.13 as colored points indicative of resultant signal strength. The green and red transmitter icons indicate actual and estimated AP source locations, respectively. The result of the test site data for this method is discussed in chapter 8.X.

Figure 7.5.13 – Array Intersections and Source Prediction

7.3. Collection Drive Path

In order to make a direct comparison between collection methods, it is important that data is collected from identical locations on the test site. For the stationary methods in which the vehicle is stopped during collection, specific points for each site were chosen. The same is true for the mobile collection methods, except rather than choosing stationary points; a specific drive path was defined. To minimize the possibility of antenna interference altering test results, the tests were not performed simultaneously. However, because these collection points were strictly adhered to, the difference in location at the analysis level is a function of GPS accuracy.

CHAPTER 8

RESULTS

8.1. Stationary Omnidirectional Results

The following presents the accuracy of the collection method described in section 7.2. The error for each of the test sites is shown in table 8.1.1 as the distance in meters between the actual transmitter and its estimated location. In figures 8.1.1 – 8.1.15, range estimates made by specific propagation models are indicated by red circles around the stationary collection points.

error (m)				
Propagation Model	**Ag. Hall**	**Connell St.**	**The Links**	**mean error (m)**
Cost 231 Urban	61.1	16.3	38.5	**38.6**
Cost 231 Suburban	64.2	10.9	48.1	**41.0**
Hata Urban	68.8	9.12	60.3	**46.0**
George Mason	66.3	49.3	58.3	**57.9**
Hata Suburban	111.8	97.67	177.9	**129.1**
Hata Rural	597.8	1056.8	1389	**1014.5**
Freespace	76111	501400	230832	**269447.6**

Table 8.1.1 – Stationary Omnidirectional Propagation Model Error

The Cost 231 urban, Cost 231 suburban, and Hata urban models produced similar results, which are expected to some extent considering their path loss similarity, as shown in figure 7.2.3. The George Mason path loss matches closely with these for a loss of between 110-120 dB. However, losses outside this interval produce significantly different range estimates than the Hata urban and both Cost 231 models. Such is the case for the Connell St. site, shown in figure 8.1.11, where signal strength measurements at a single location yielded a total loss of greater than 120 dB. This caused an overestimate of range

for that location which significantly impacted the overall error. The poor results for the Freespace, Hata suburban, and Hata rural models are due to the severe overestimates in range that each typically produces. As these range estimates become large with respect to the separation between measurement points, inaccuracies associated with the collinear point problem discussed in section 3.2 begin to take effect.

In general, the range estimates for the Ag. Hall test site were very inaccurate. The Cost 231, George Mason, and Hata urban models significantly underestimated range for this open area test site, as shown in figures 8.1.1 – 8.1.4. Conversely, the Freespace and Hata rural models, shown in figure 8.1.6 and 8.1.7, greatly overestimated range.

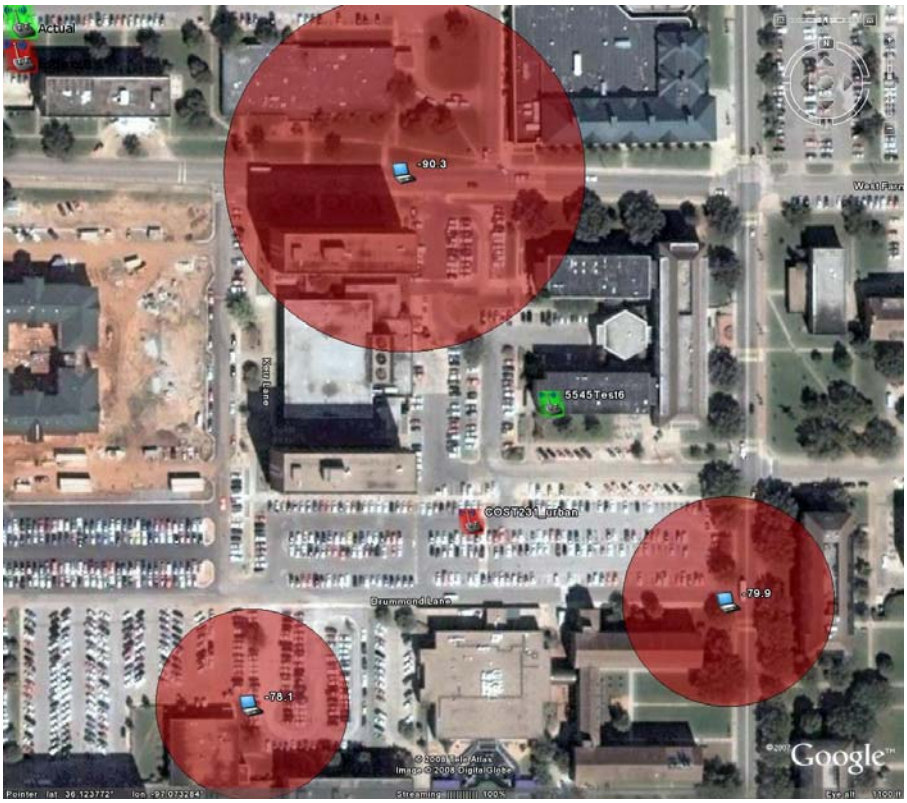

Figure 8.1.1 –Stationary Cost 231 Urban for Ag. Hall Site

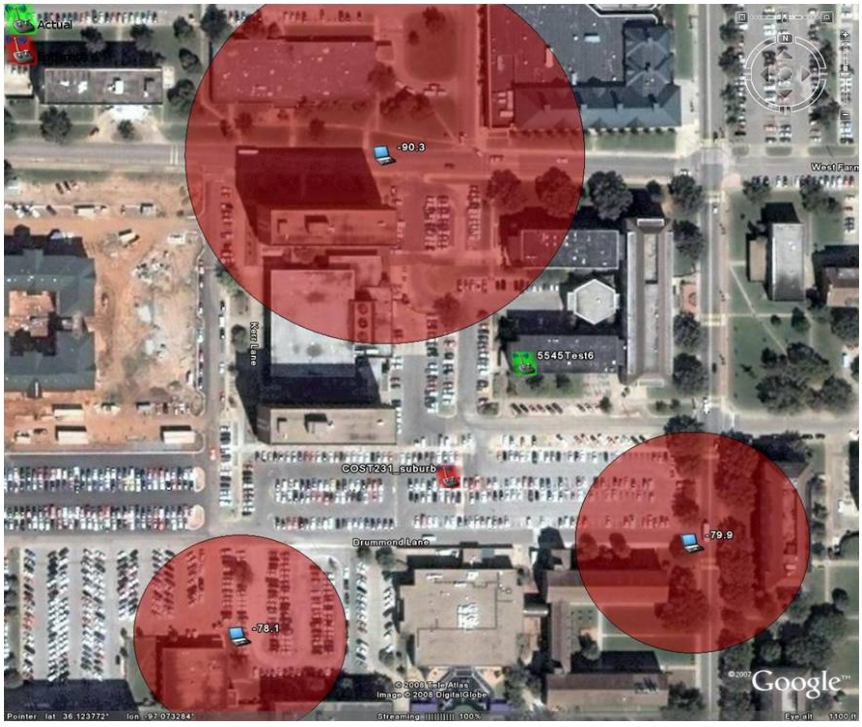

Figure 8.1.2 –Stationary Cost 231 Suburban for Ag. Hall Site

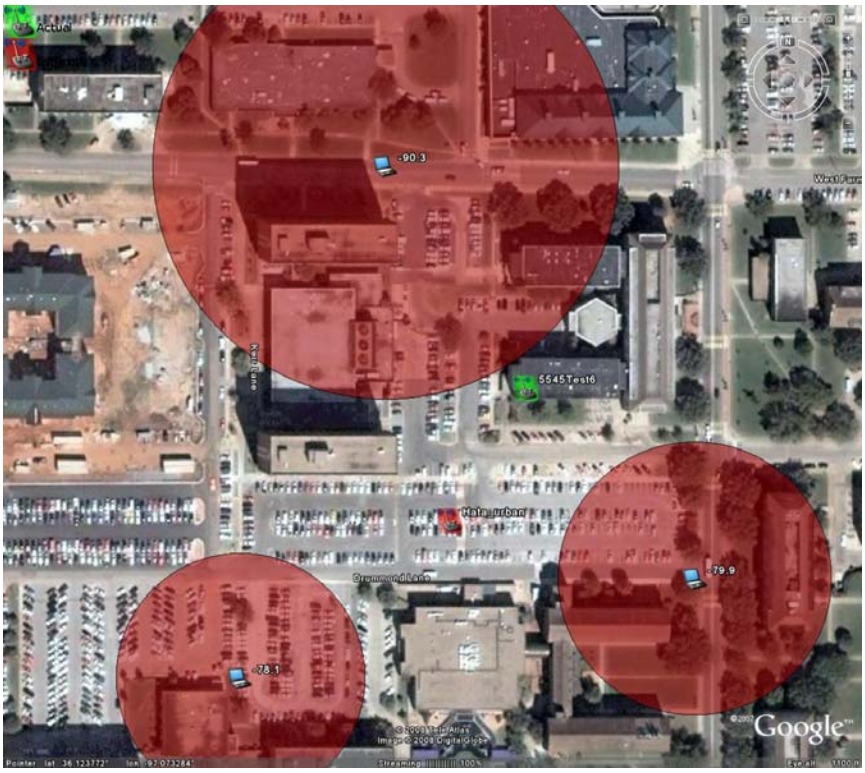

Figure 8.1.3 –Stationary Hata Urban for Ag. Hall Site

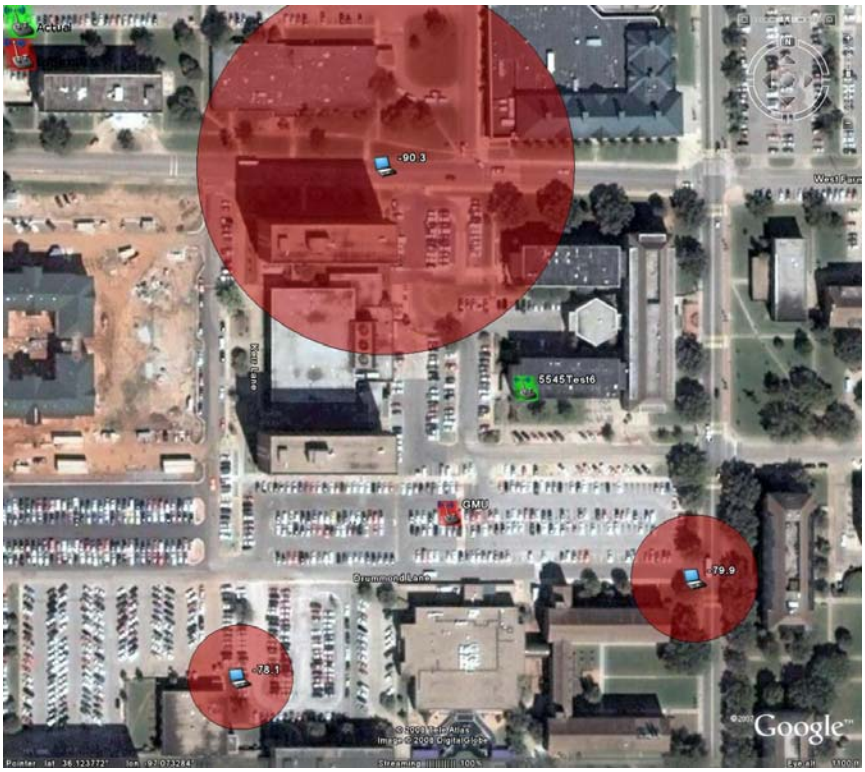

Figure 8.1.4 –Stationary GMU for Ag. Hall Site

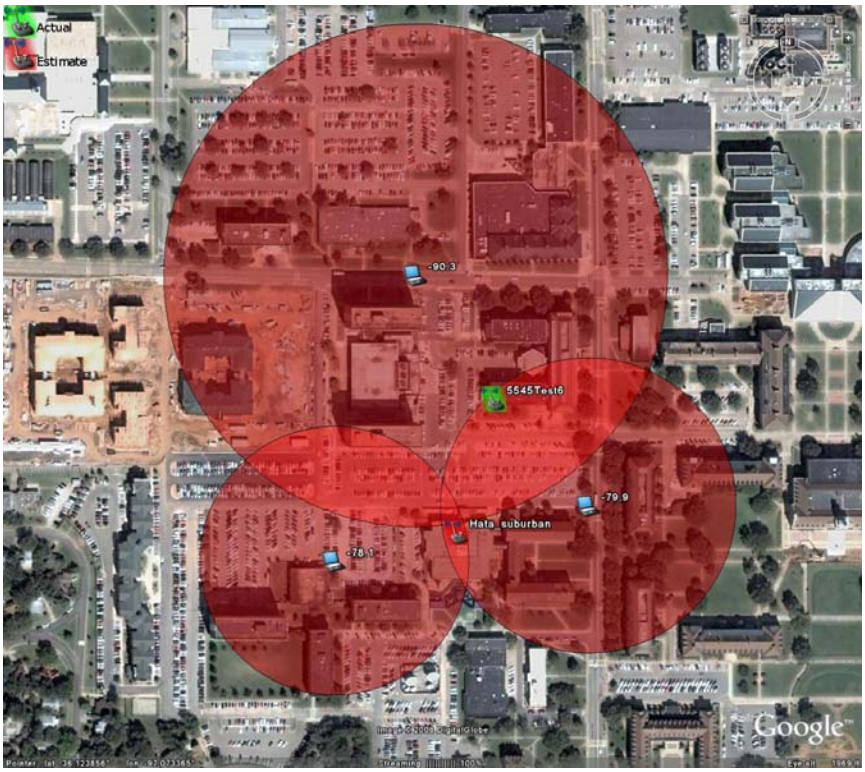

Figure 8.1.5 –Stationary Hata Suburban for Ag. Hall Site

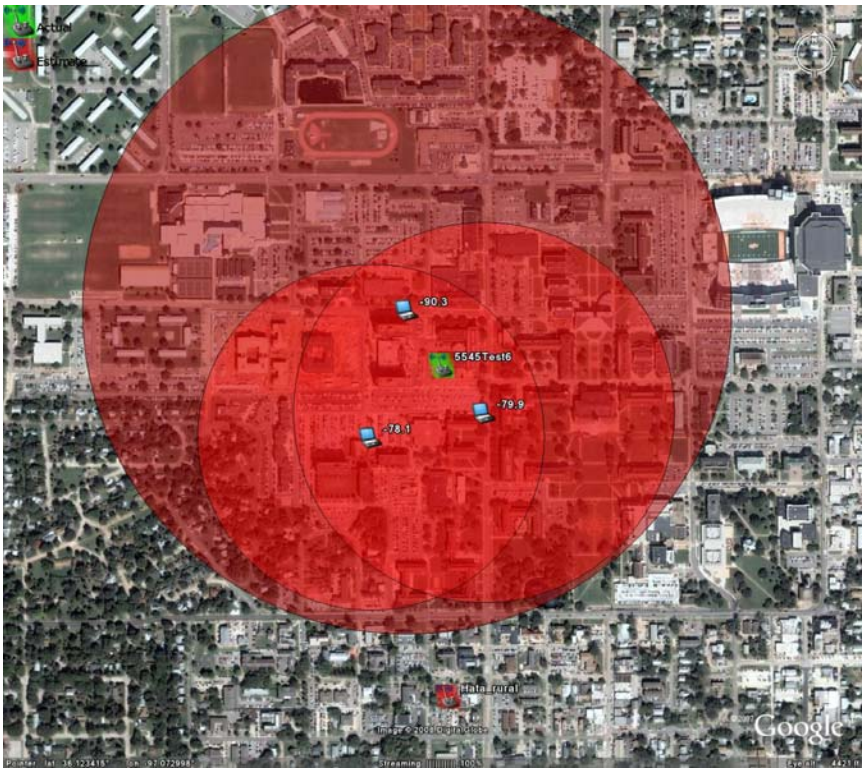

Figure 8.1.6 –Stationary Hata Rural for Ag. Hall Site

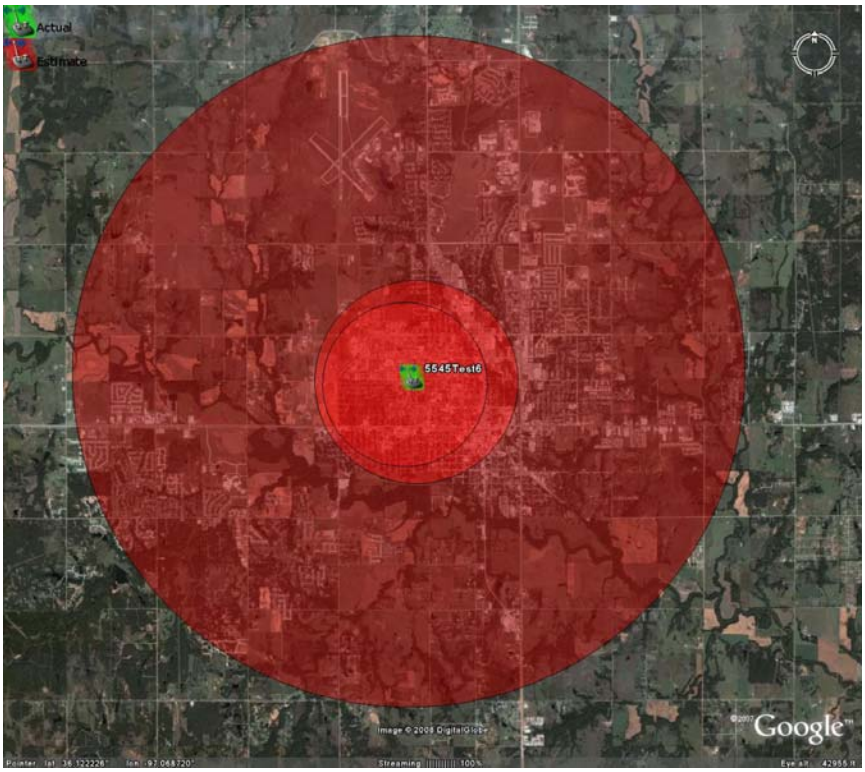

Figure 8.1.7 –Stationary Freespace for Ag. Hall Site

The Cost 231 urban, Cost 231 suburban, and Hata urban models produced very accurate range estimates for the Connell St. test site. The George Mason model also produced accurate range estimates, but only for three of four measurement locations. One range was significantly overestimated, thus it is less accurate than the other three models. Figures for the Hata suburban, Hata rural, and Freespace models for this site are left out due to excessive range overestimation.

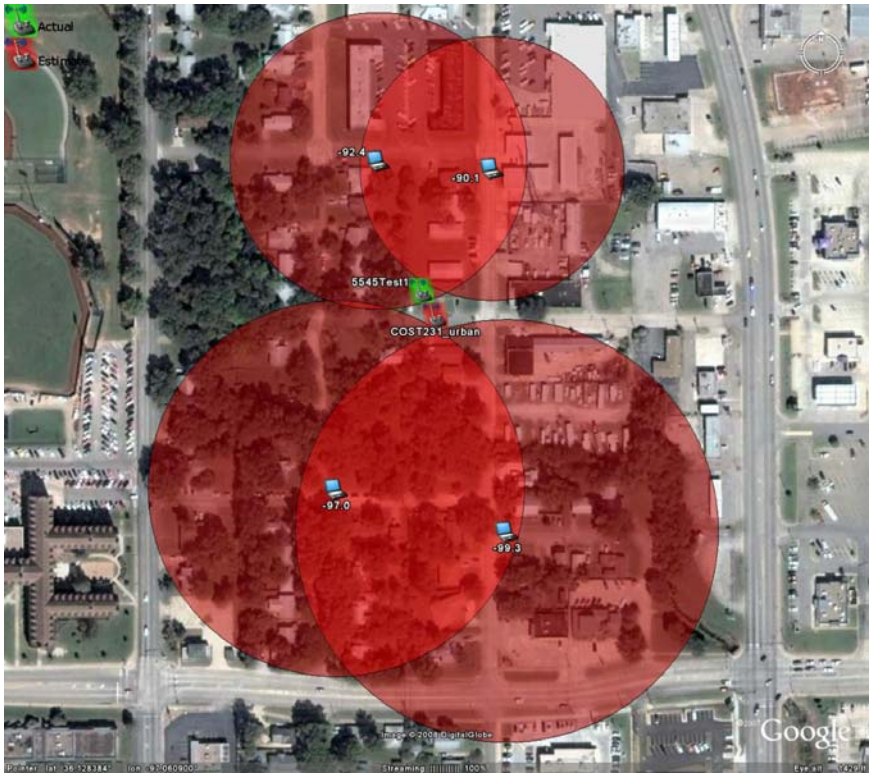

Figure 8.1.8 –Stationary Cost 231 Urban for Connell St. Site

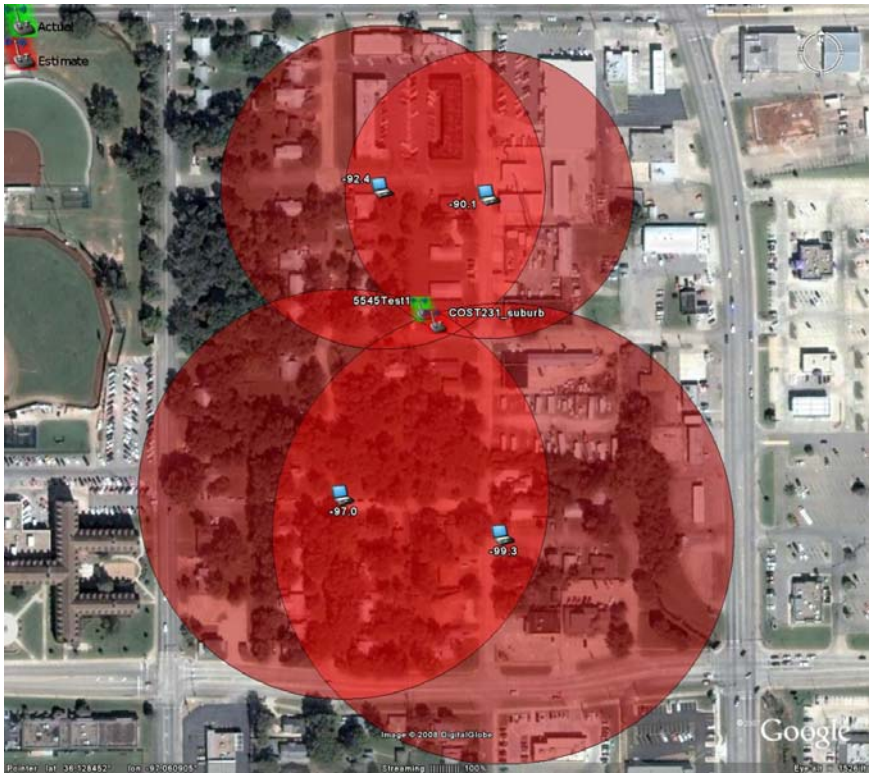

Figure 8.1.9 –Stationary Cost 231 Suburban for Connell St. Site

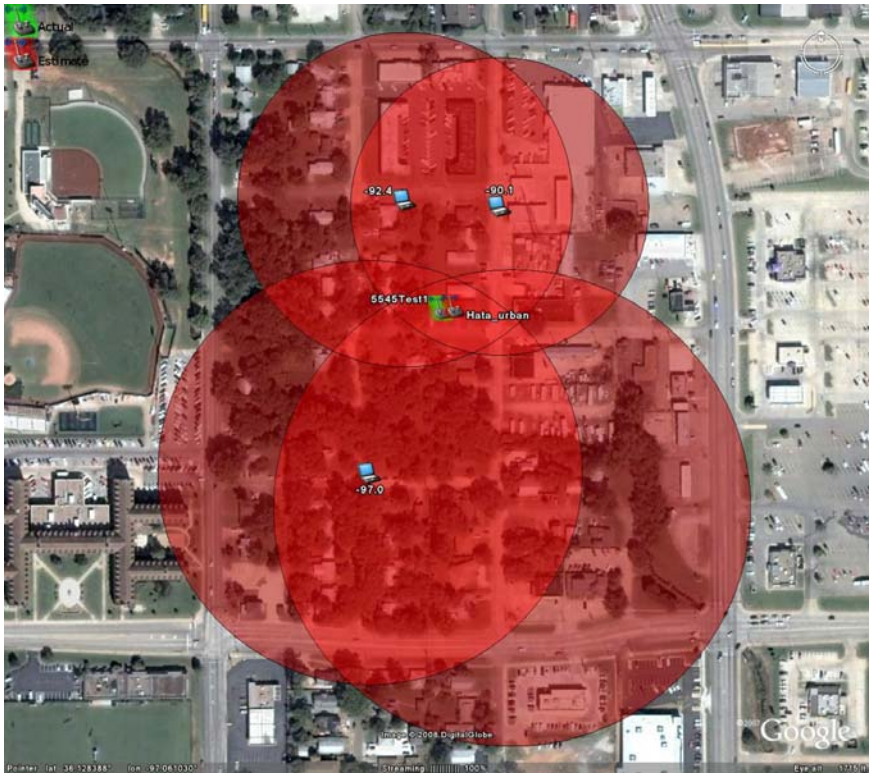

Figure 8.1.10 –Stationary Hata Urban for Connell St. Site

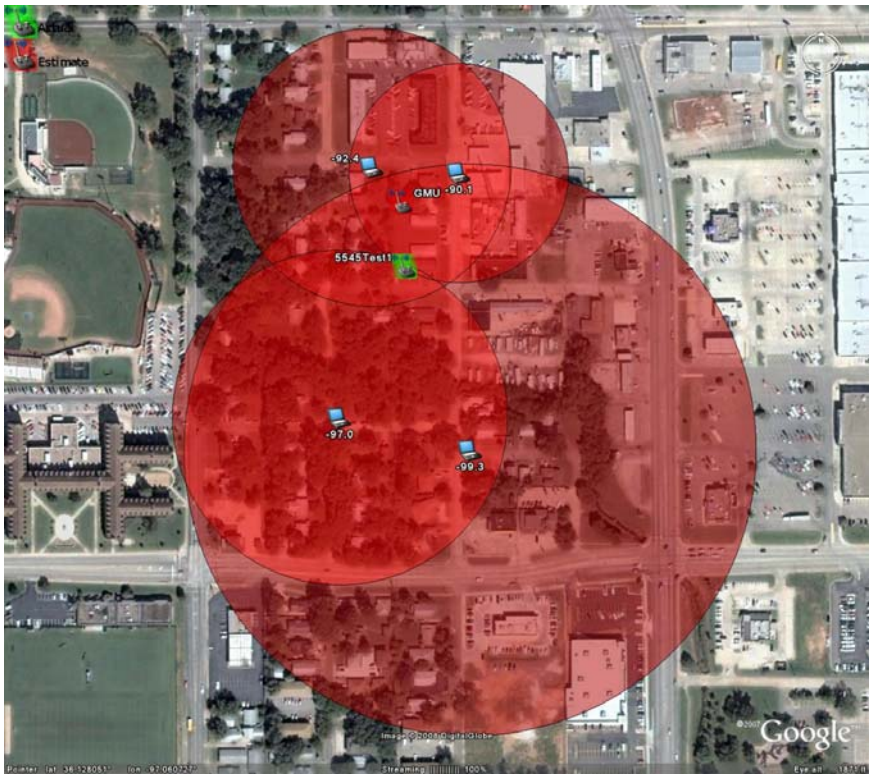

Figure 8.1.11 –Stationary GMU for Connell St. Site

At the Links test site, the results were poor considering the close proximity of which the measurements were taken. With the exception of the George Mason model, ranges estimates for the collection points on the left side of figure 8.1.12 were reasonably accurate. However, estimates for the collection point on the right side of figure 8.1.12 were consistently overestimated, which was the main cause for such inaccurate source location estimates.

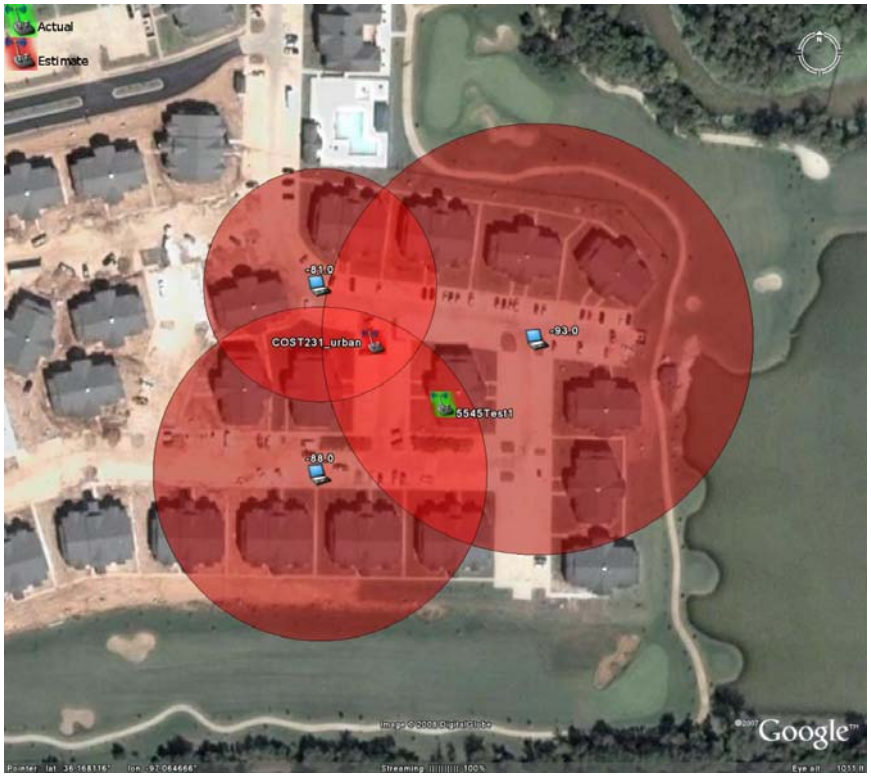

Figure 8.1.12 –Stationary Cost 231 Urban for Links Site

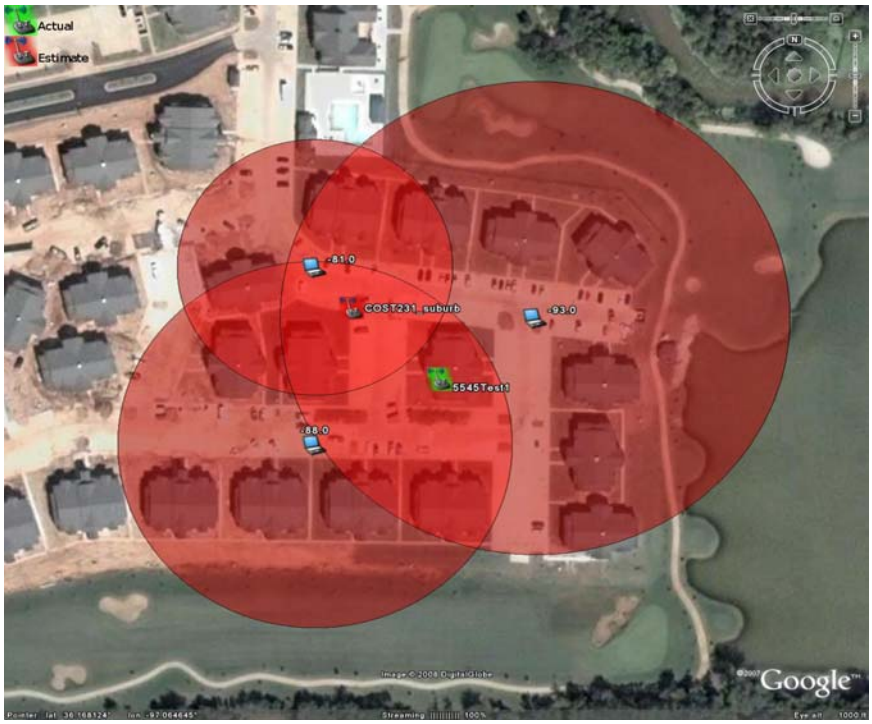

Figure 8.1.13 –Stationary Cost 231 Suburban for Links Site

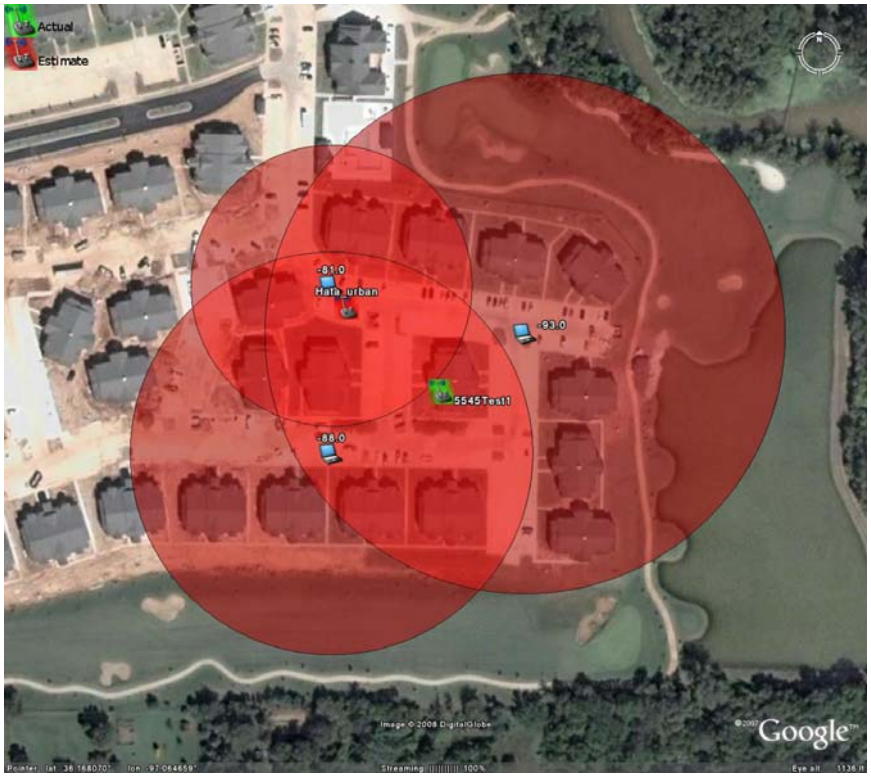

Figure 8.1.14 –Stationary Hata Urban for Links Site

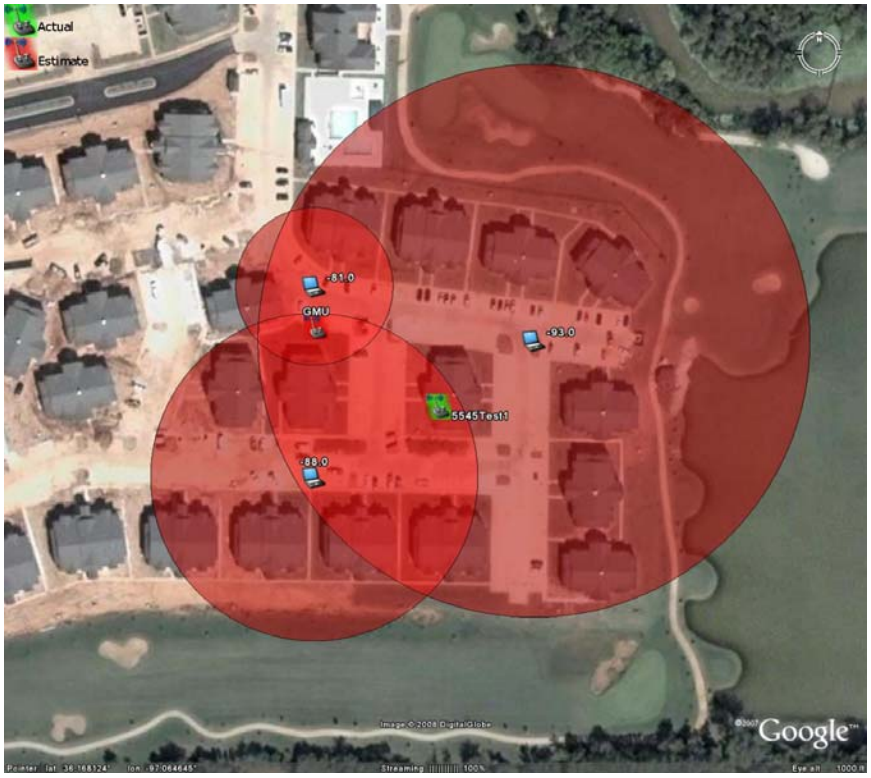

Figure 8.1.15 –Stationary GMU for Links Site

8.2.1. Mobile Omnidirectional Results

The results of the test method described in section 7.2, which utilizes omnidirectional collection while in motion, indicate significantly more accurate results for the Ag. Hall and Links test sites. However, the results for Connell St. were much less accurate for the mobile case, likely due to the many propagation obstacles included on the site.

error (m)				
Propagation Model	**Ag. Hall**	**Connell St.**	**The Links**	**mean error (m)**
Cost 231 Urban	29.4	54.9	24.8	**36.4**
Cost 231 Suburban	35.2	50.5	23.9	**36.6**
Hata Urban	44.2	45.2	27.9	**39.1**
George Mason	70.6	25.3	33.7	**43.2**
Hata Suburban	141.7	47.8	101.6	**74.7**
Hata Rural	1170	523	1388	**955.5**
Freespace	174389	198982	231087	**215034.5**

Table 8.2.1 - Mobile Omnidirectional Propagation Model Error

Figures 8.2.1, 8.2.3, and 8.2.5 show the Cost 231 urban range estimates for signal strength measurements taken for each of the three test sites. Figures 8.2.2, 8.2.4, and 8.2.6 show the corresponding RSSI measurements vs. geographic separation from the transmitter. The blue curve in these figures is indicative of the fast fading that occurs as a result of a signal that traverses multiple paths in route to the receiver. This can result in either constructive or destructive interference which will significantly affect overall signal strength over small changes in distance. This is shown in the figures, as the blue curve can change by as much as 15dB over distances as short as 1m. The black curve is a

linear regression fit to the data in attempt to find an average path loss vs. distance for each site.

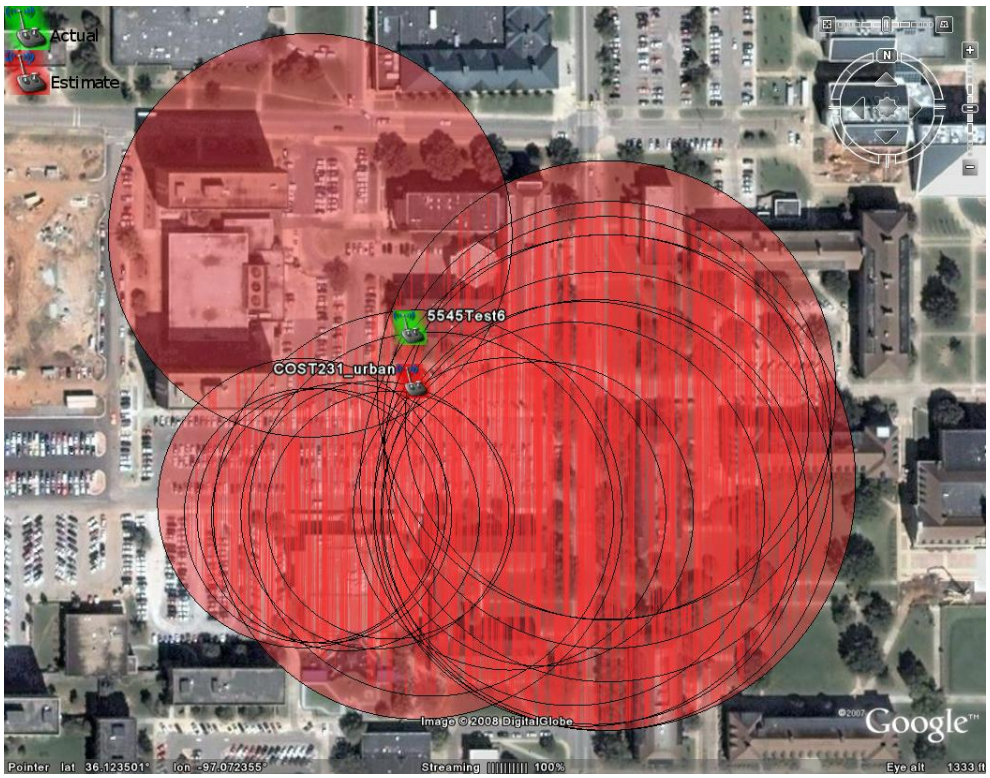

Figure 8.2.1 –Mobile Cost 231 Urban for Ag. Hall Site

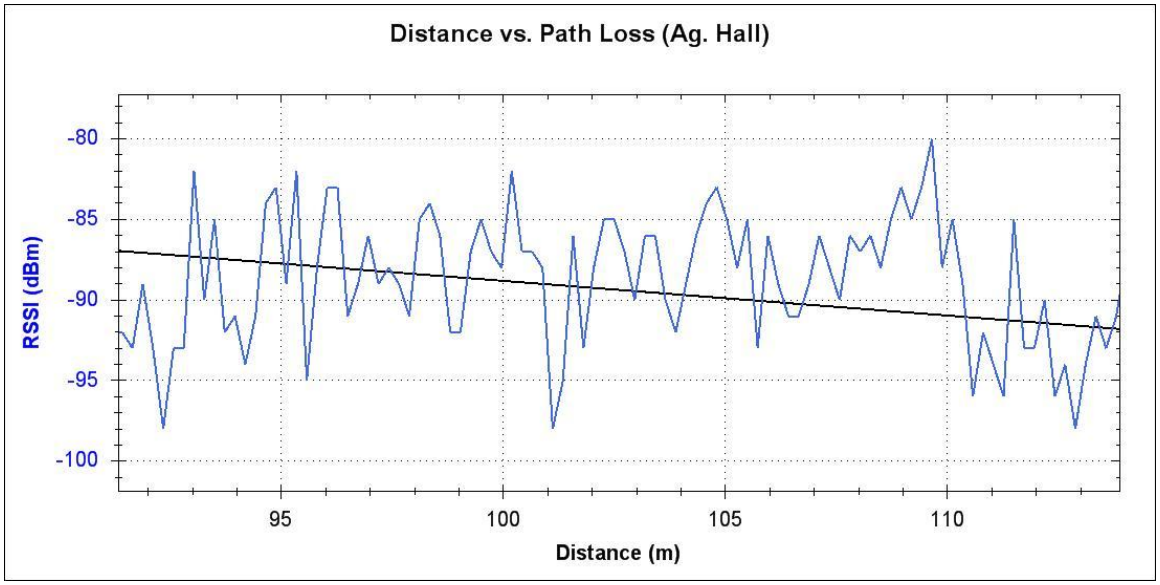

Figure 8.2.2 – Fading for Ag. Hall Site

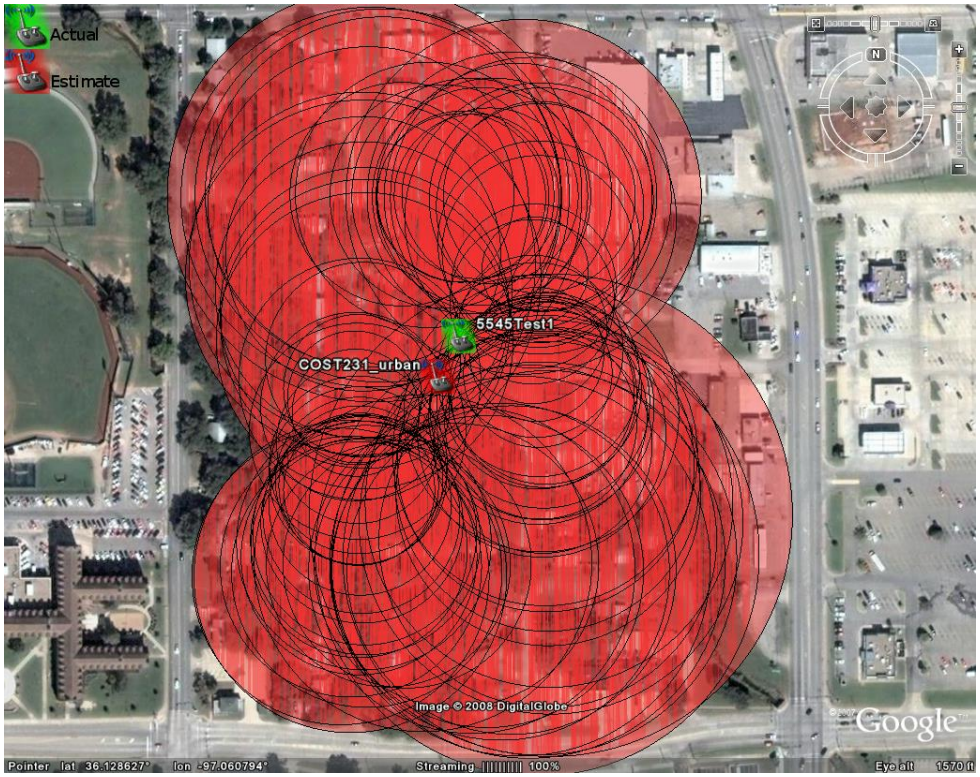

Figure 8.2.3 –Mobile Cost 231 Urban for Connell St. Site

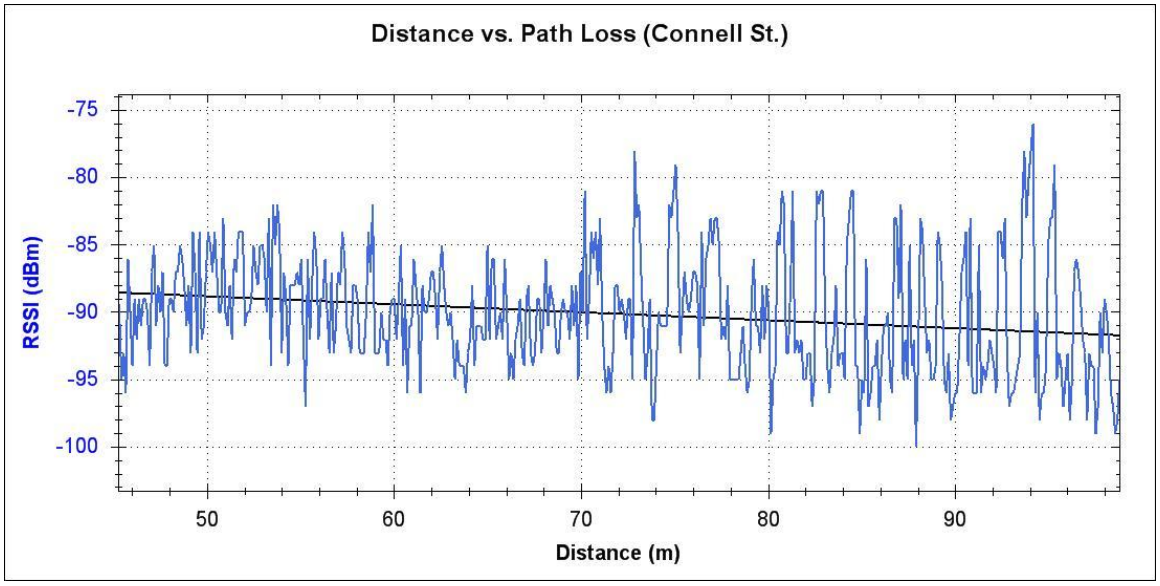

Figure 8.2.4 – Fading for Connell St. Site

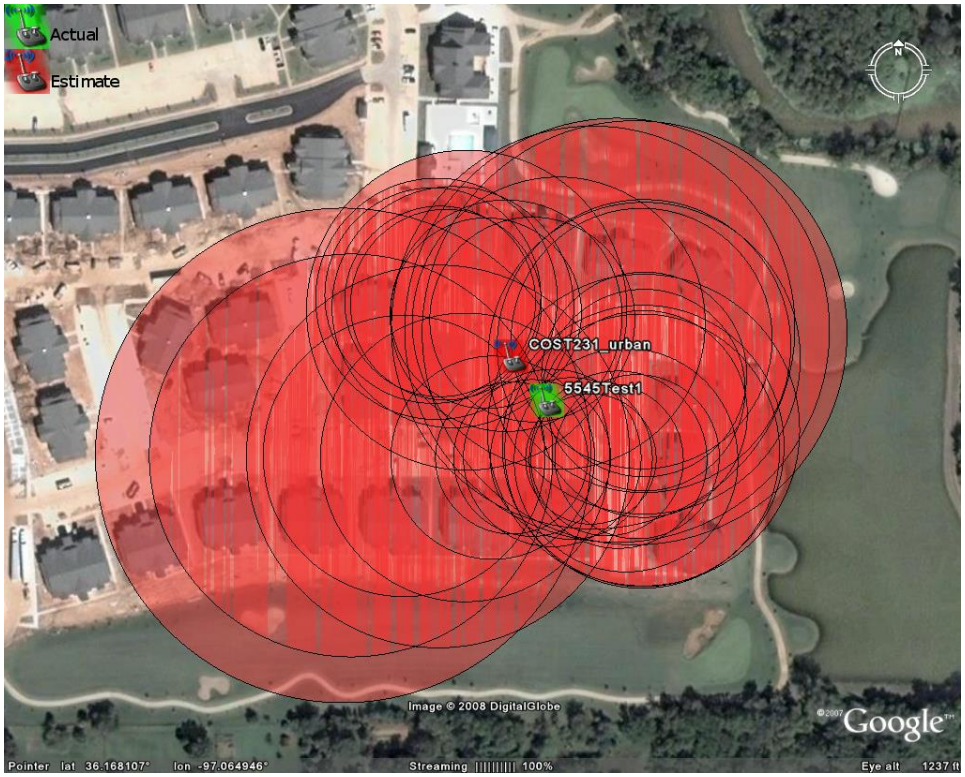

Figure 8.2.5 –Mobile Cost 231 Urban for Links Site

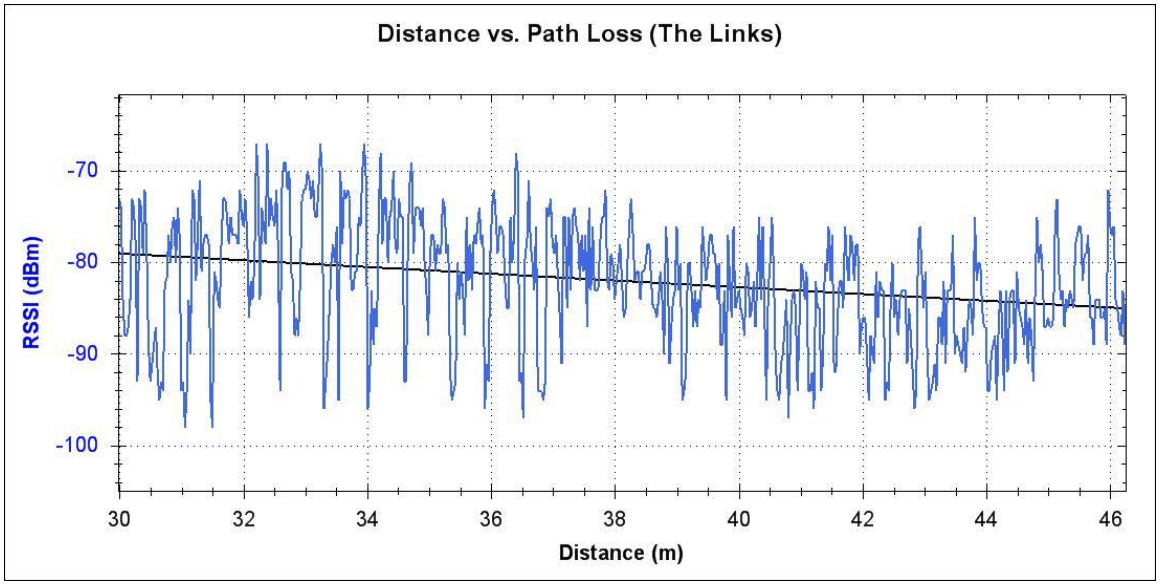

Figure 8.2.6 – Fading for Links Site

8.3. Stationary Scanning Directional Results

Table 8.3.1 shows the results of the stationary, mechanically scanned directional antenna method described in section 7.4. This technique proved to be much more accurate and consistent than either omnidirectional collection method. For each site, the HG2414P produced noticeably more accurate results than the lower gain, less directional HG2409P antenna. An investigation to determine if an antenna with even higher directionality produces more accurate results is left as future work.

Test Site	**HG2409P**	**HG2414P**
Ag. Hall	20.3	12.3
Connell St.	29.9	23.2
The Links	32.8	13.2
mean error (m)	**27.6**	**16.2**

Table 8.3.1 - Stationary Scanning Directional Error

Figures 8.3.1 through 8.3.6 shows scan data collected at each site for both the HG2409P and HG24014P antennas. The legend centered on top of each figure shows the relationship between color and RSSI, where red is maximum signal strength and blue is minimum. The green lines that extend beyond the beam pattern for each point is the peak value that resulted from the iterative peak comparison described in section 7.4.

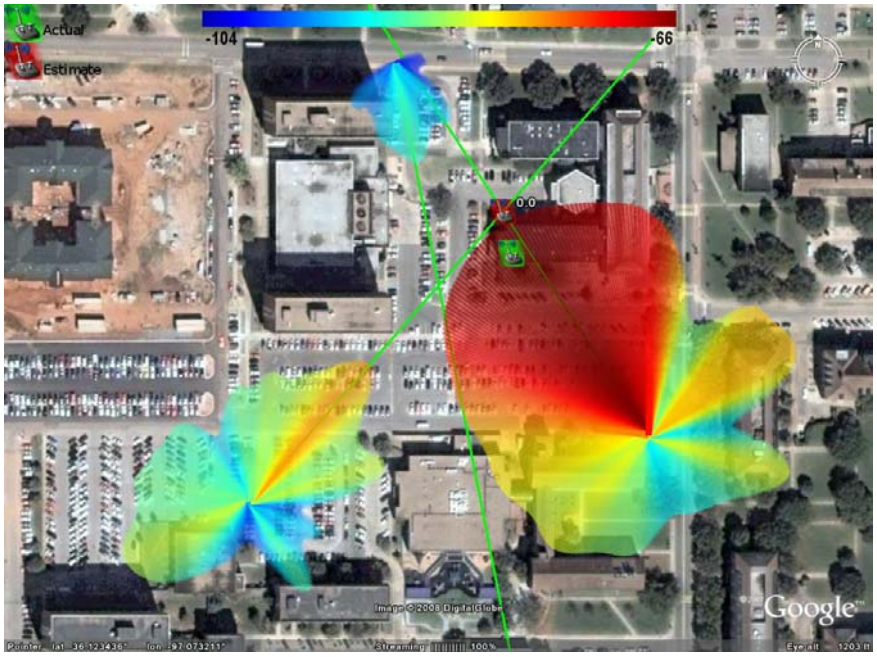

Figure 8.3.1 –Stationary HG2409P Scan for Ag. Hall Site

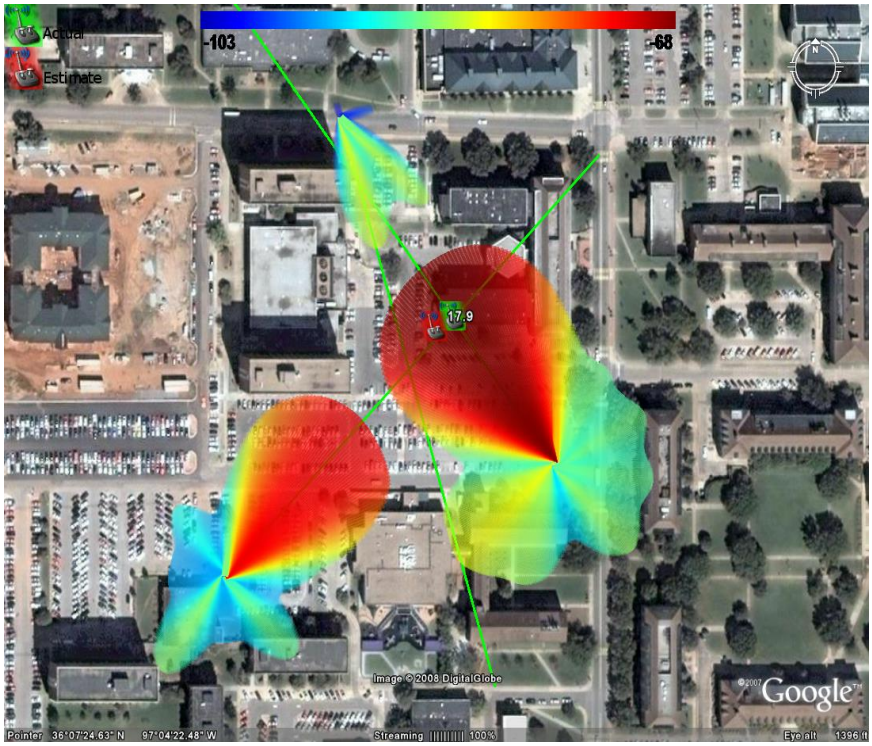

Figure 8.3.2 –Stationary HG2414P Scan for Ag. Hall Site

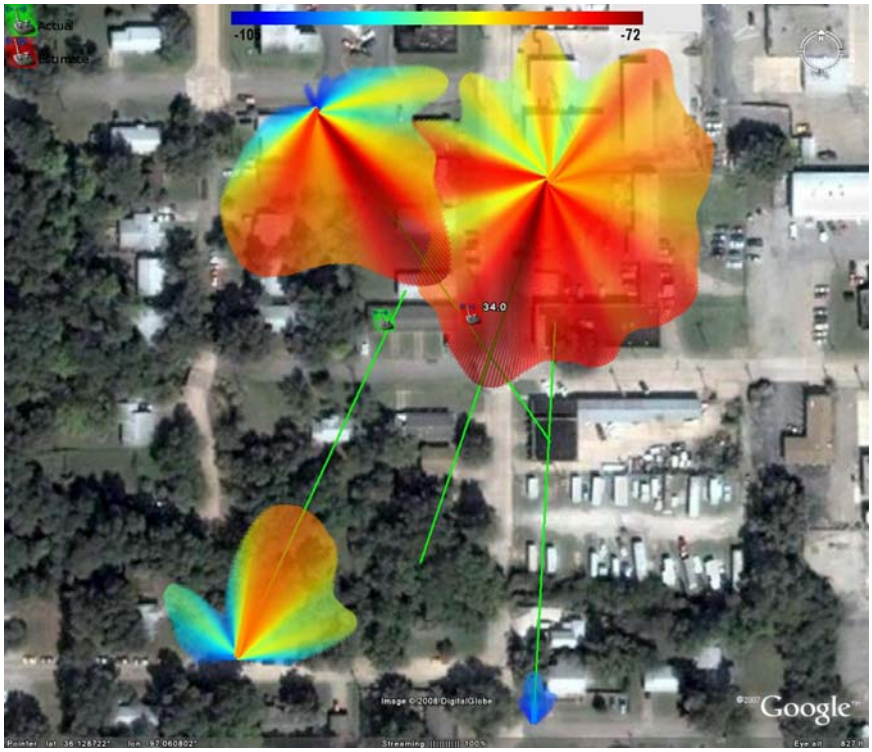

Figure 8.3.3 –Stationary HG2409P Scan for Connell St. Site

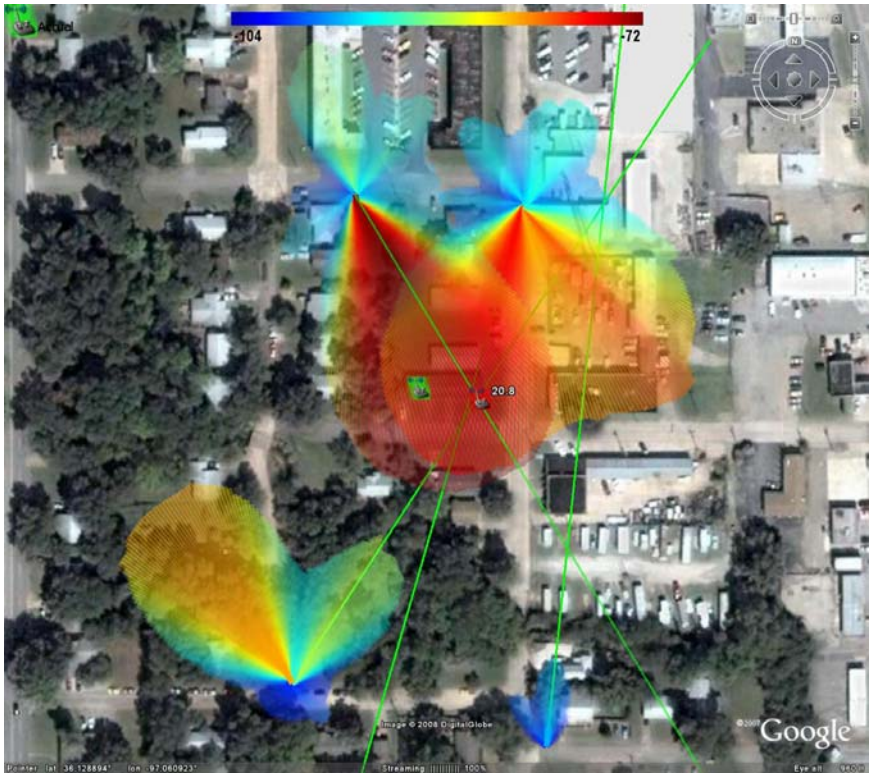

Figure 8.3.4 –Stationary HG2414P Scan for Connell St. Site

Figure 8.3.5 –Stationary HG2409P Scan for Links Site

Figure 8.3.6 –Stationary HG2414P Scan for Links Site

8.4. Mobile Directional Array Results

The accuracy of the final method, which simultaneously collects data from four directional antennas while in motion, is shown in table 8.4.1. Similar to the previous section, the more directional, higher gain HG2414P antenna produced better results than the broader beamwidth HG2409P. Although data was collected from many more points around each test site, this method was on average less accurate then the stationary scanned array discussed in section 8.3. However, it was much more accurate and consistent than either omnidirectional based method.

	HG2409P	**HG2414P**
Ag. Hall	45.5	29.9
Connell St.	9.6	17.3
The Links	14.2	5.4
mean error (m)	**23.1**	**17.7**

Table 8.4.1 - Mobile Directional Array Error

In order to maintain a manageable overall size, an array of only four patch antennas was used, each spaced 90º apart. As stated previously, elements consisted of either HG2409P or HG2414P antennas, which have horizontal half power beam widths of 75º and 30º, respectively. Multiplying these values by four to account for each antenna yields a number less than 360º, which means that sections exist on the horizontal plane that are outside the antenna's half power beam width. These areas are shown by the white circles in figures 8.4.1 and 8.4.2 for the HG2409P and HG2414P antennas, respectively. Due to the low antenna gain in these areas, much lower signal strength is produced when one of these areas is pointing toward the transmitter. This is especially apparent for the

HG2414P, which possesses as much as 20 dB of attenuation in these areas. This produces attenuated signal strength values not indicative of source location.

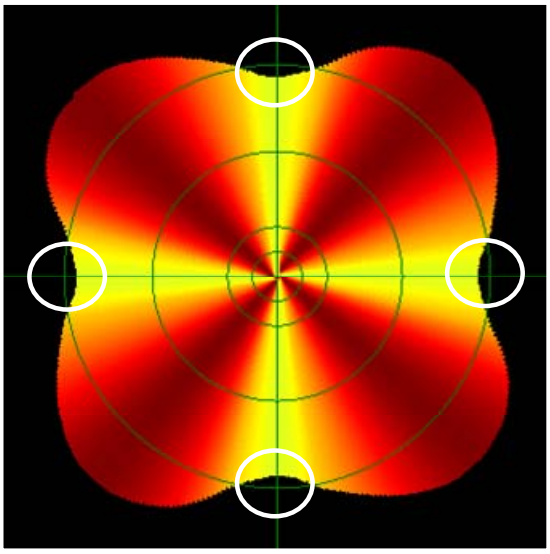

Figure 8.4.1 – HG2409P Mobile Array Pattern Holes

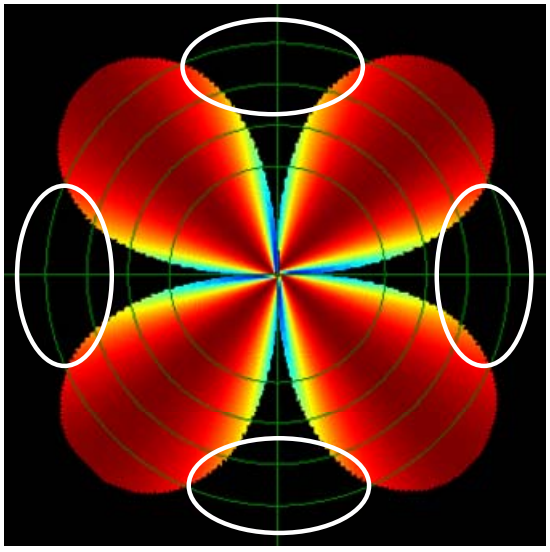

Figure 8.4.2 – HG2414P Mobile Array Pattern Holes

Figures 8.4.3- 8.4.14 shows data collected at each site for both directional antennas. For each instance, the raw data is shown as well as the results of the filtering and analysis routine described in section 7.5. For each individual vector, color and length are indicative of average signal strength for that particular location.

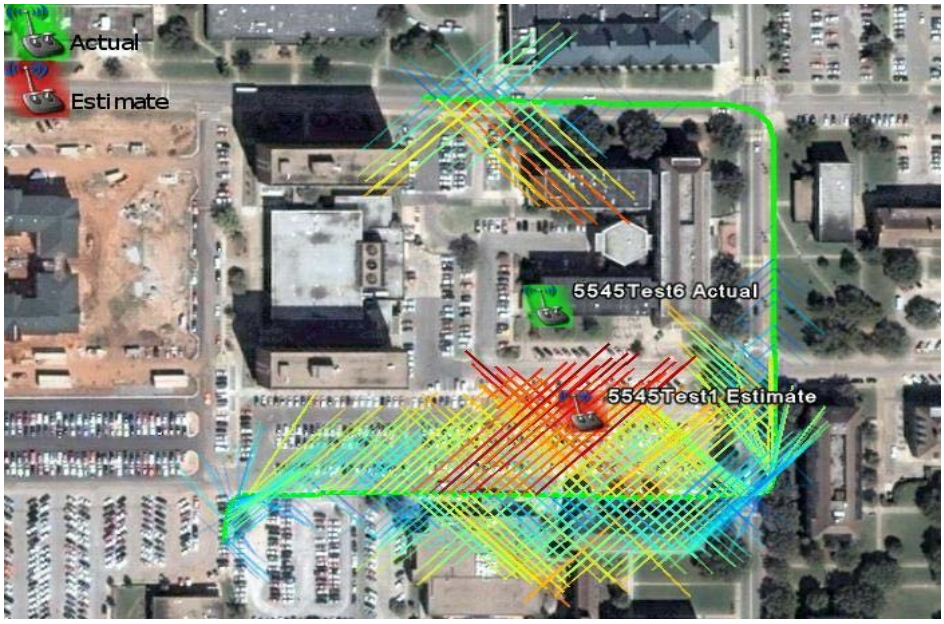

Figure 8.4.3 – HG2409P Mobile Array Raw Data for Ag. Hall Site

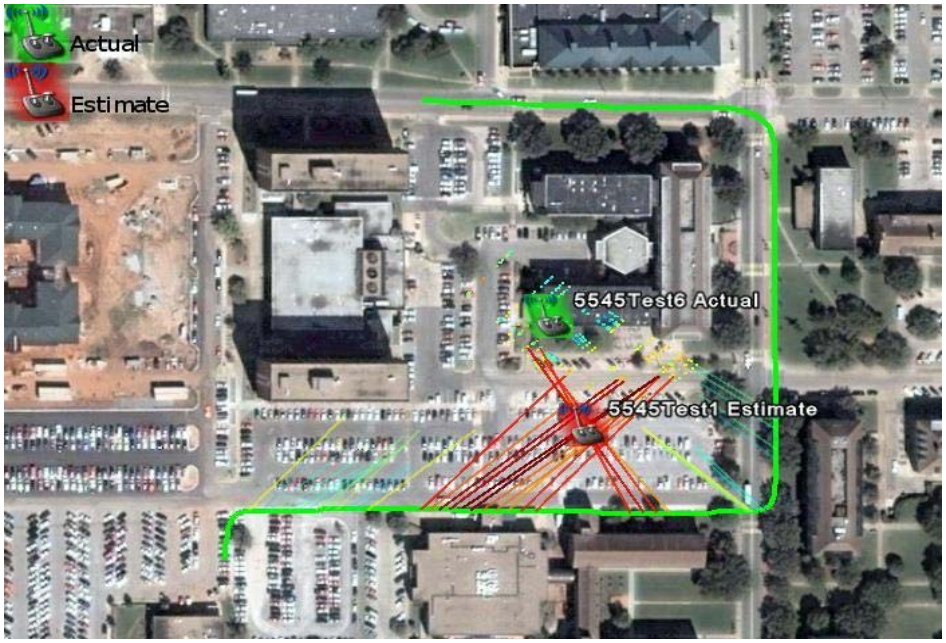

Figure 8.4.4 – HG2409P Mobile Array Filtered Data for Ag. Hall Site

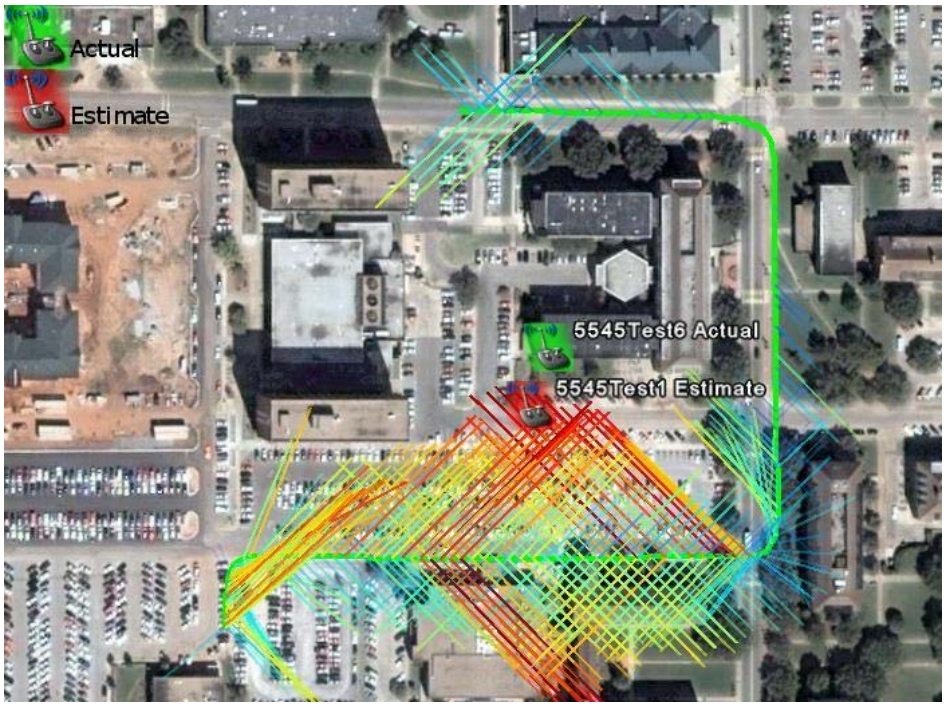

Figure 8.4.5 – HG2414P Mobile Array Raw Data for Ag. Hall Site

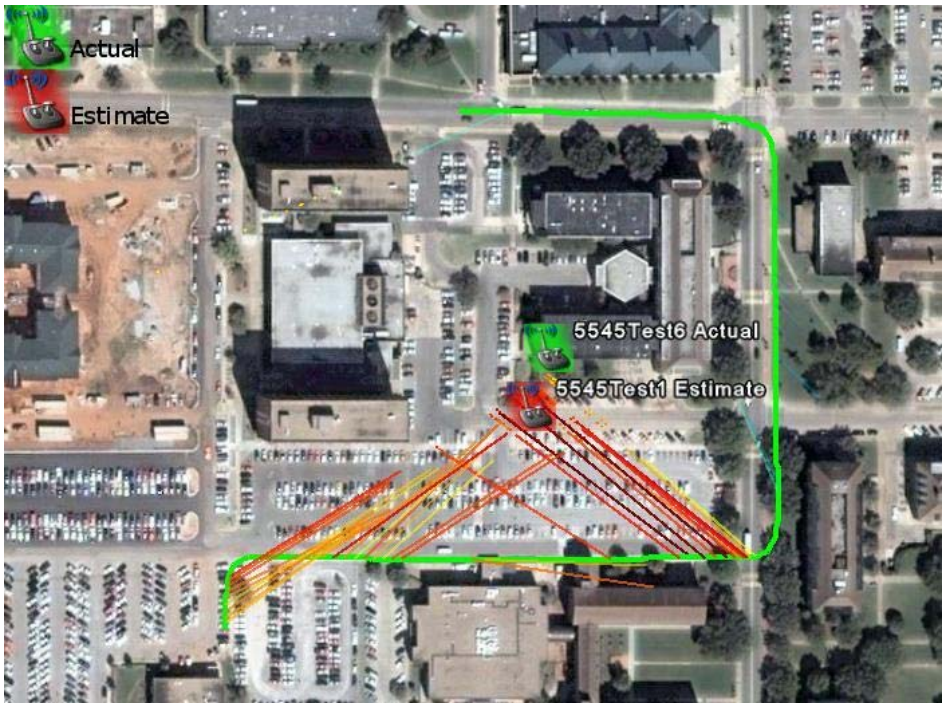

Figure 8.4.6 – HG2414P Mobile Array Filtered Data for Ag. Hall Site

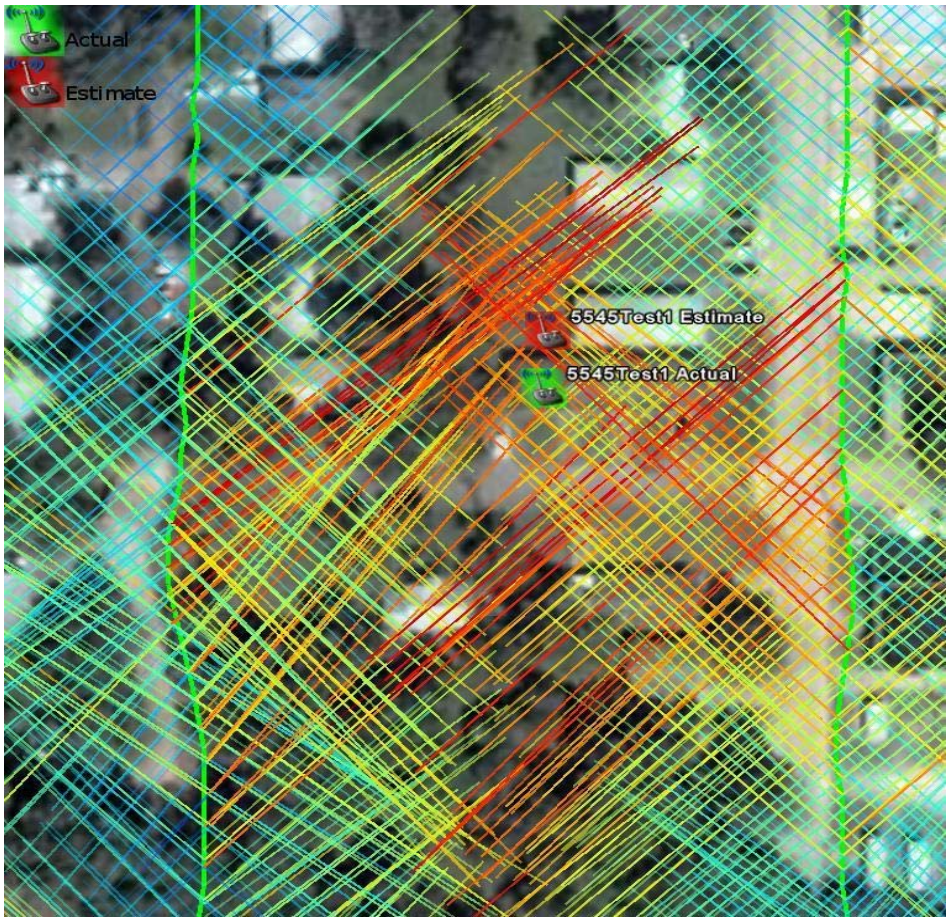

Figure 8.4.7 – HG2409P Mobile Array Raw Data for Connell St. Site

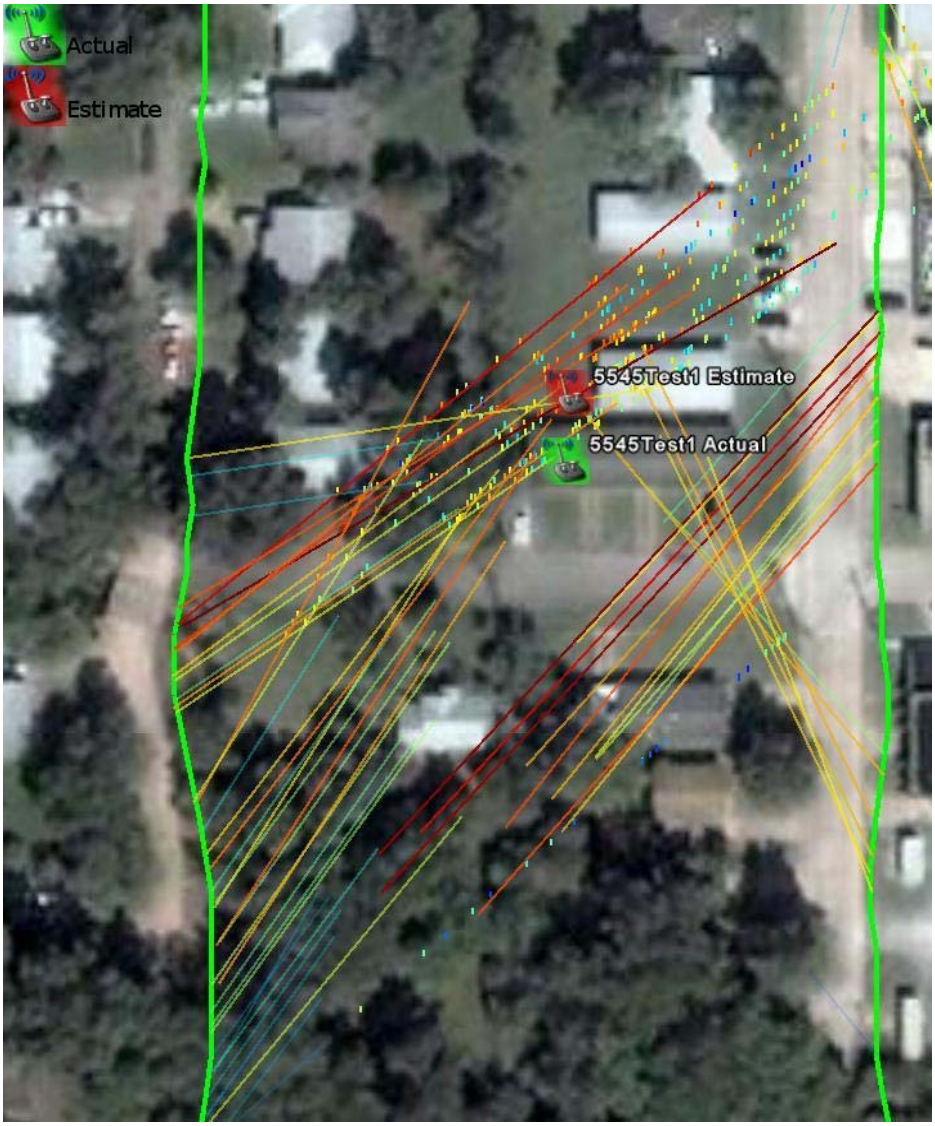

Figure 8.4.8 – HG2409P Mobile Array Filtered Data for Connell St. Site

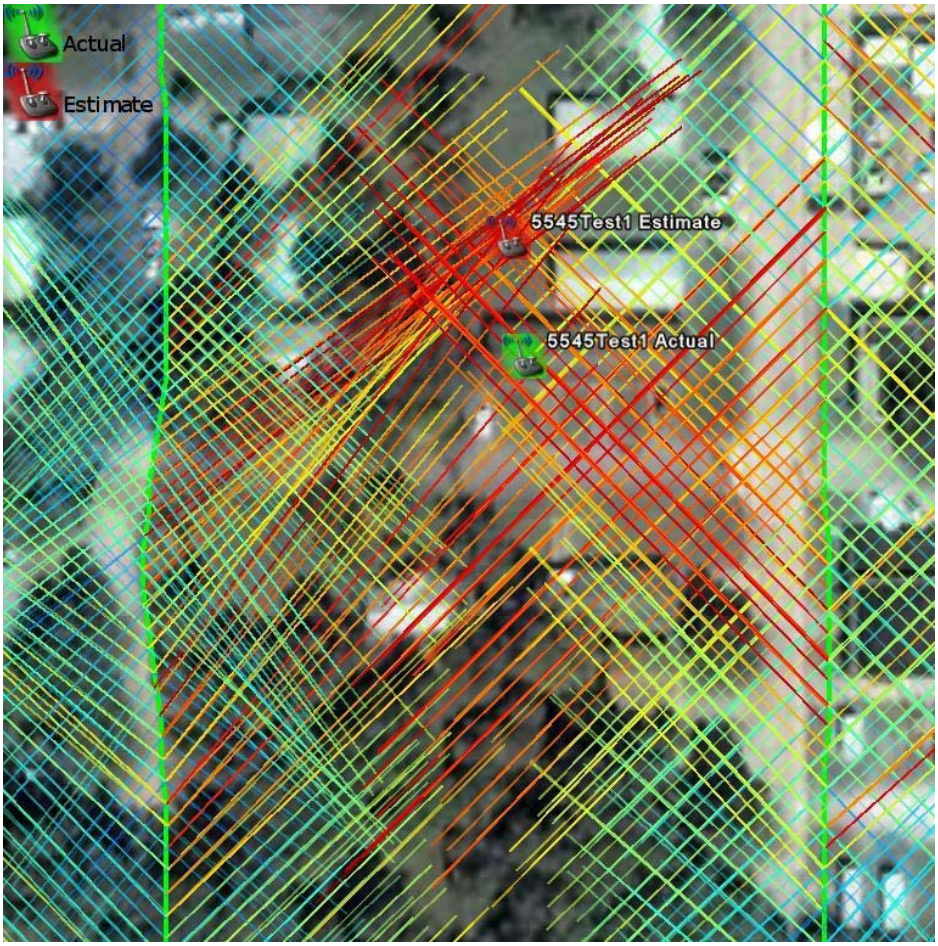

Figure 8.4.9 – HG2414P Mobile Array Raw Data for Connell St. Site

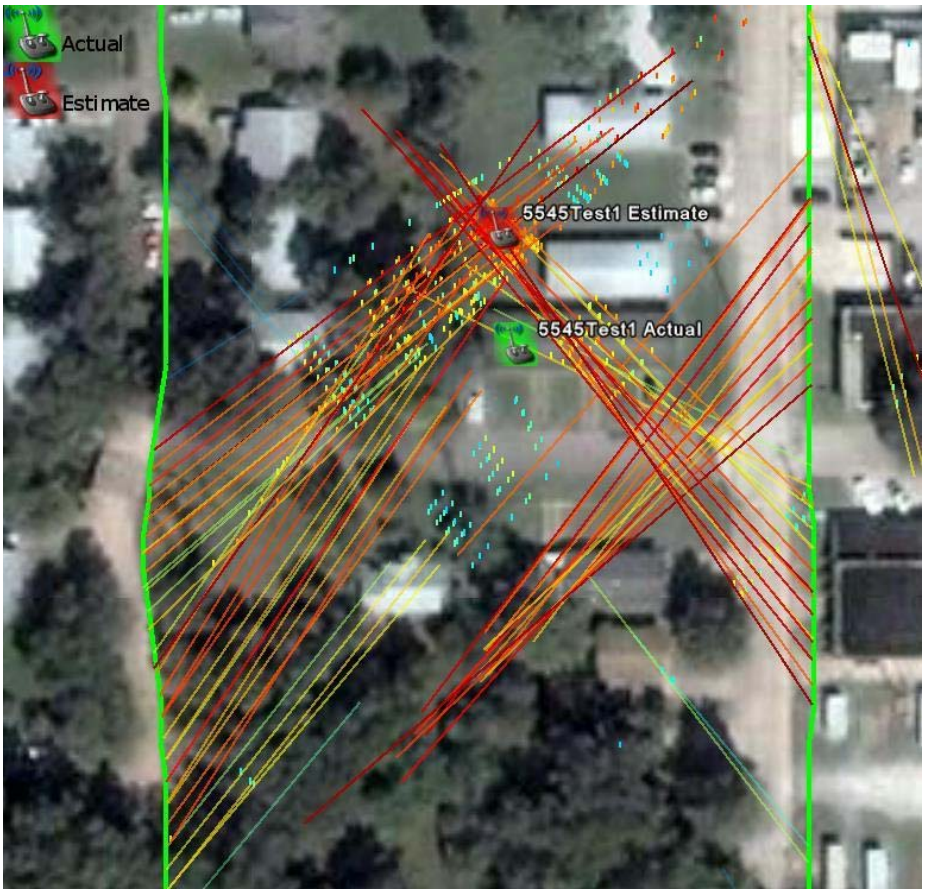

Figure 8.4.10 – HG2414P Mobile Array Filtered Data for Connell St. Site

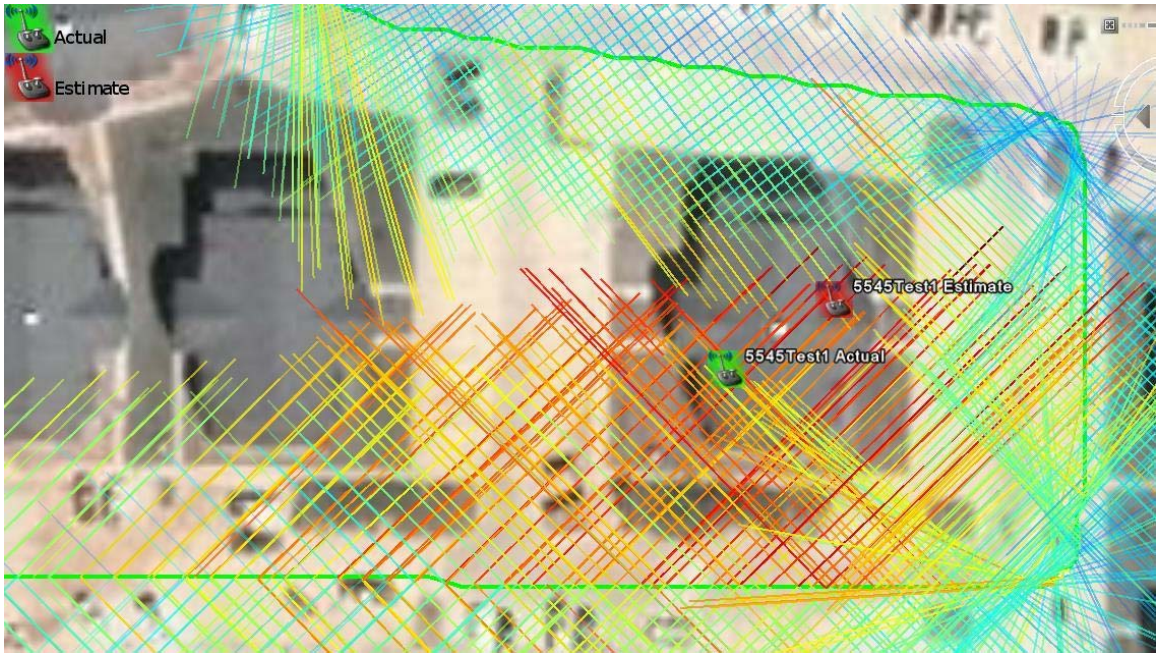

Figure 8.4.11 – HG2409P Mobile Array Raw Data for Links Site

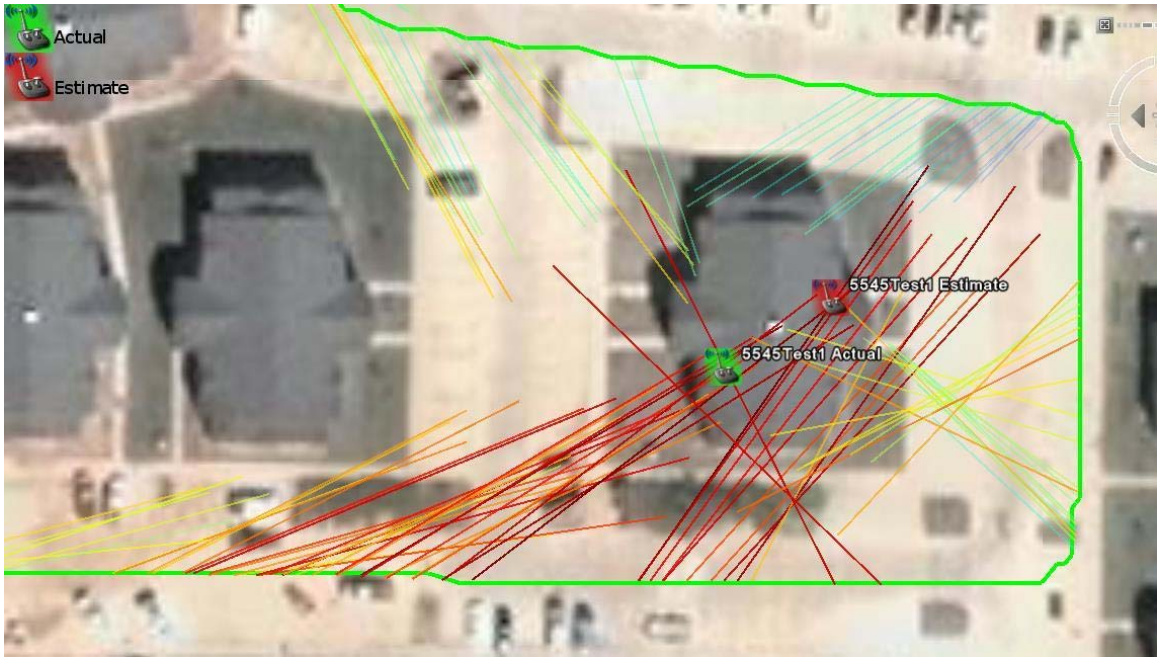

Figure 8.4.12 – HG2409P Mobile Array Filtered Data for Links Site

Figure 8.4.13 – HG2414P Mobile Array Raw Data for Links Site

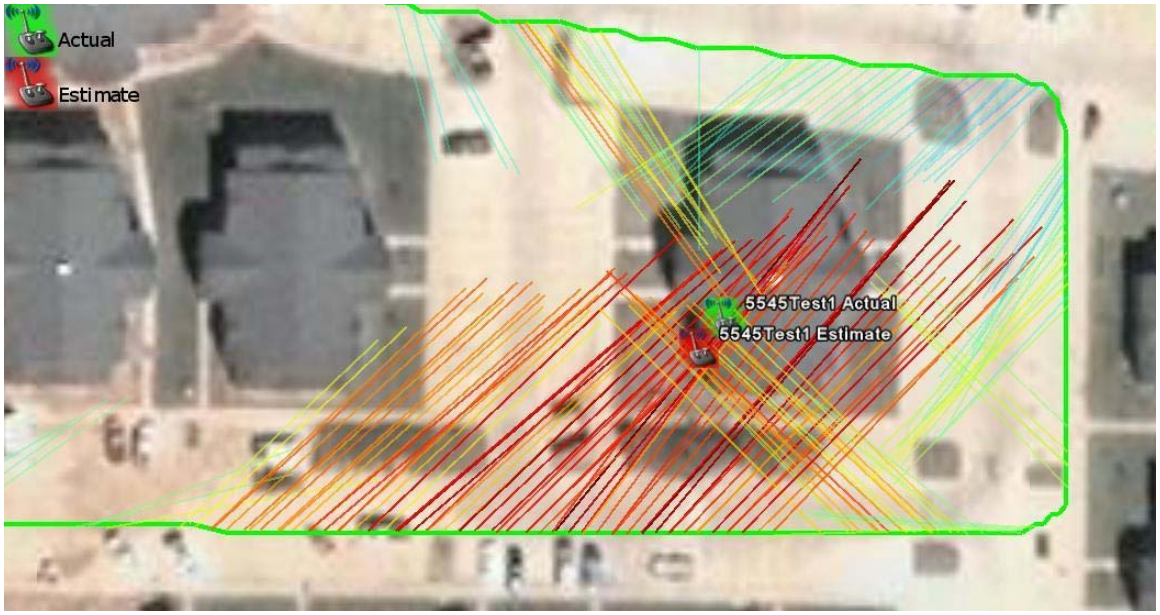

Figure 8.4.14 – HG2414P Mobile Array Filtered Data for Links Site

CHAPTER 9

Linear Collections

Chapter 8 shows estimation results in which received signal strength measurements were made from multiple points surrounding the AP. However, this type of collection may not always be possible due to the absence of roads or environmental obstructions. This chapter discusses estimates resulting from a linear collection path.

9.1 Range Based Estimates Resulting from Linear Collection

When using multilateration to compute the source estimate of range based systems, the axes perpendicular to a linear collection path displays significant error due to perpendicular intersection lines, as discussed in section 3.2. In figures 9.1.1 and 9.1.2, for instance, although the propagation model produced very accurate range estimates, the source estimates show significant error. Note that the estimate for figure 9.1.1 is located outside of the area in the display. This problem makes multilateration an ineffective technique for localization given linear collection data.

If multilateration is removed from the analysis and the data is simply inspected visually, the ability to pick a source estimate remains difficult. The symmetric nature of the range intersections with respect to the collection path will likely yield two equally likely estimates, shown in figure 9.1.3 and 9.1.4.

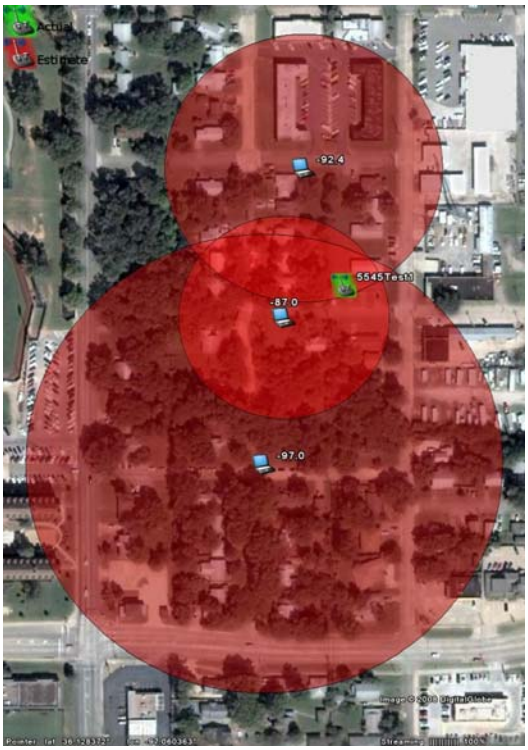

Figure 9.1.1 – Stationary Linear Range

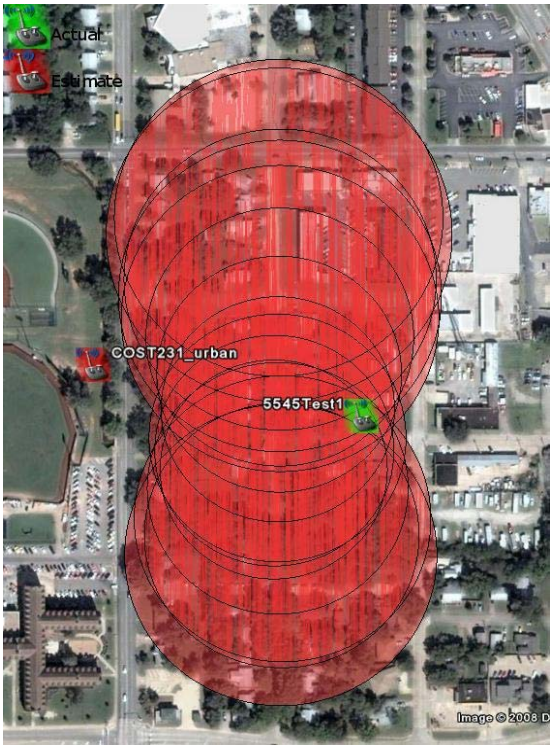

Figure 9.1.2 – Mobile Linear Range

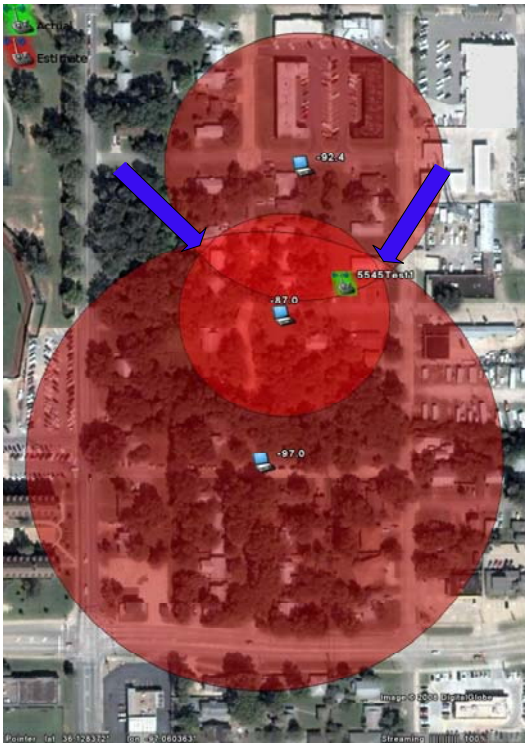

Figure 9.1.3 – Visual Estimates

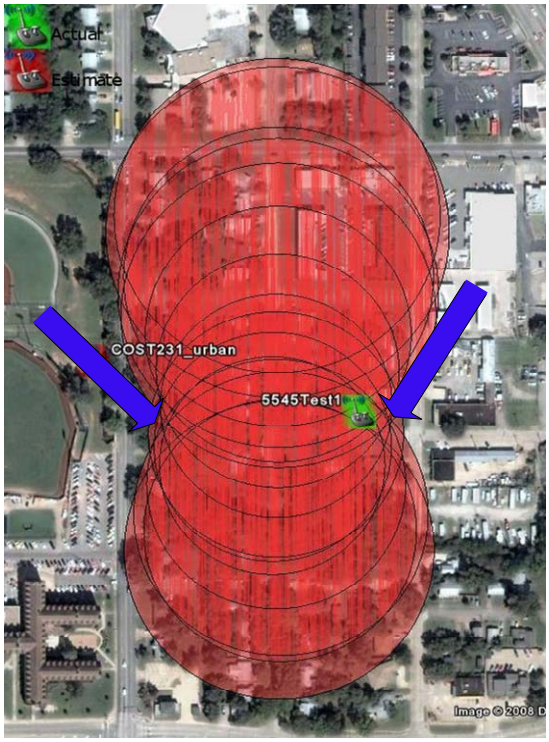

Figure 9.1.4 – Visual Estimates

9.2 AoA Based Estimates Resulting from Linear Collection

Linear data points do not have the same effect on accuracy when using AoA based systems. In fact, two AoA measurements taken on collinear points can provide a very accurate source estimate, as shown in figure 9.1.3. Data collected using the mobile array method also display accurate results, as shown in Figure 9.1.4.

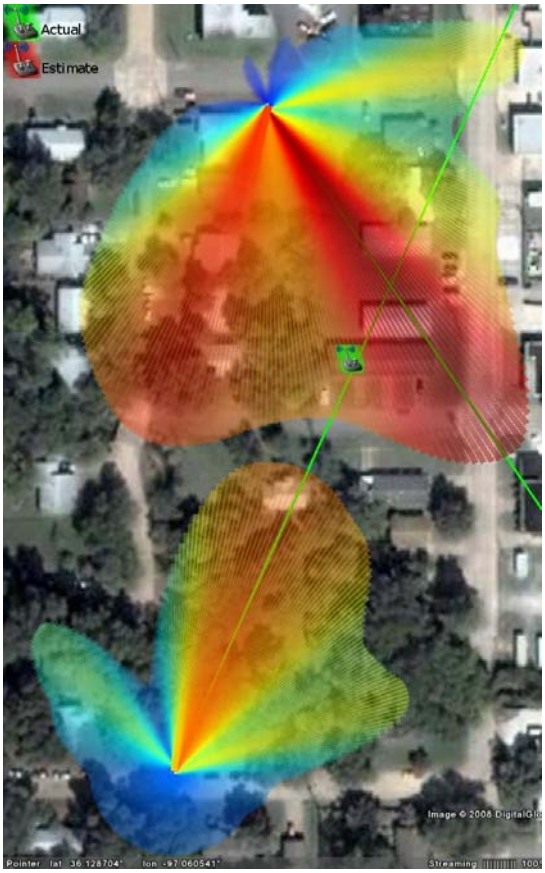

Figure 9.1.3 – Stationary Linear AoA

Figure 9.1.4 – Mobile Linear AoA

CHAPTER 10

CONCLUSION

This research has introduced and evaluated several collection methods and estimation algorithms used to localize 802.11 wireless access points. Methods utilizing directional antennas showed consistent accuracy for all locations, especially the narrower beamwidth antenna. In areas of significant multipath, the filtering and analysis techniques used by the directional methods were able to identify these reflections and compensate in order to obtain an accurate estimate.

However, the methods employing omnidirectional antennas produced inconsistent results. While the estimates were accurate for some test sites, they were highly inaccurate for the others. This is because propagation models only provide an average path loss for a generalized environment type based on empirical data. Inaccuracies in range estimates exist due to the inability to measure the variance from the average for each specific location. Due to the significance of these errors, the use of propagation models for this research was ineffective in consistently estimating transmitter location.

FUTURE WORK

The results of directional testing showed that for both the stationary and mobile collection techniques, the narrower beamwidth antenna yielded more accurate results than the wider beamed unit. Future research could extend this observation to determine if greater accuracy can be achieved with even narrower beamed antennas.

As shown in section 8.4, portions of the directional array gain fall below half power with respect to the main beam. These unequal coverage areas on the horizontal plane produce attenuated signal strength values not indicative of source location. The addition of antennas into these attenuated sections could provide increased accuracy and is recommended for future investigation.

REFERENCES

[1] T. K. Sarkar, M. Wicks, M. Palma, and R. Bonneau, *Smart Antennas.* Hoboken: Wiley and Sons, 2003.

[2] T.S. Rappaport, *Wireless Communications, Principles and Practice*. Prentice-Hall, 2002.

[3] C. Smith, D. Collins, *3G Wireless Networks*. McGraw-Hill*, 2001.*

[4] H.R. Anderson, *Fixed Broadband Wireless System Design.* Hoboken: Wiley and Sons, 2003.

[5] N. Osifchin and G. Vau, "3D Ultrasonic Tagging System for Observing Human Activity," *Intelligent Robots and Systems, 2003*, pp. 785-791.

[6] H. Senturk, "Performance Evaluation of Hyperbolic Position Location Technique in Cellular Wireless Networks," B.S. thesis, Air Force Institute of Technology, WPAFB, OH, 2002.

[7] P.K. Sagiraju, P. Gali, D. Akopian, and G.V. Raju, "Enhancing Security in Wireless Networks Using Security Techniques," *System of Systems Engineering, 2007.* pp. 1-6.

[8] P. Bahl and V.N. Padmanabham. "RADAR: An In-Building RF-Based User Location and Tracking System," *INFOCOM 2000.* pp. 775-784.

[9] M. Robinson and I. Psaromiligkos, "Received Signal Strength Based Location Estimation of a Wireless LAN Client," *Wireless Communications and Networking Conference,* 2005. pp. 13-17.

[10] V.S. Abhayawardhana, I.J. Wassell, D. Crosby, M.P. Sellars, M.G. Brown, "Comparison of Empirical Propagation Path Loss Models for Fixed Wireless Access Systems," *Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st*, vol.1, pp. 73-77 Vol. 1, 30 May-1 June 2005

[11] M. Heidari, "A Testbed for Real-Time Performance Evaluation of RSS-based Indoor Geolocation Systems in Laboratory Environment", M.S. thesis, Worcester Polytechnic Institute, 2005.

[12] "Propagation Losses Through Common Building Materials, 2.4GHz and 5GHz," 07-15-2002, [on-line], available from www.am1.us/Papers/E10589%20Propagation%20Losses%202%20and%205GHz.pdf; Internet; accessed 11-15-2007.

[13] P. H. Dana, “Global Positioning System Overview,” [on-line], available from http://www.colorado.edu/geography/gcraft/notes/gps/gps.html; Internet; accessed 12-10-2007.

[14] “Log Distance PL with Shadowing,” [on-line], available from www.coe.montana.edu/ee/andyo/EE447/EE44707_L12-14.pdf; Internet; accessed 11-02-2007.

[15] IEEE Std 802.11-1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[16] "RF Basics: Part 1," 04-14-2007, [on-line], available from https://edge.arubanetworks.com/article/rf-basics-part-1; Internet; accessed 10-21-2007.

[17] H. Stark, J. Woods, *Probability, Random Processes, and Estimation Theory for Engineers*. Prentice-Hall, 1994.

[18] A. Allen, *Probability, Statistics, and Queuing Theory with Computer Science Applications.* Academic Press, 1990.

[19] GMU Communications and Networking Lab, (2007). *Characterization of Wireless Channels, Phase 2 Report.* Unpublished work.

[20] “Butterfly Wi-Fi Power Meter,” [on-line], available from http://www.bvsystems.com/Products/Power/Butterfly/butterfly.htm; Internet; accessed 10-21-2007.

[21] “Linksys WRT54G Series,” [on-line], available from http://en.wikipedia.org/wiki/WRT54G; Internet; access 10-21-2007.

[22] “HG2409P Wireless Lan Antenna,” [on-line], available from http://www.hyperlinktech.com/web/hg2409p.php; Internet, 10-22-2007.

[23] “HG2414P Wireless Lan Antenna,” [on-line], available from http://www.hyperlinktech.com/web/hg2414p.php; Internet, 10-22-2007.

[24] “AirPcap Ex,” [on-line], available from http://www.cacetech.com/products/airpcap-ex.htm; Internet; accessed 10-20-2007.

[25] “AR5005UX,” [on-line], available from http://www.atheros.com/pt/AR5005UX.htm; Internet; accessed 10-20-2007

VITA

Kellen Mitchell Harwell

Candidate for the Degree of

Master of Science

Thesis: A COMPARISON OF 802.11 WIRELESS TRANSMITTER LOCALIZATION TECHNIQUES

Major Field: Electrical Engineering

Biographical:

Education: Graduated from Fayetteville High School, Fayetteville, Arkansas in May 2001; received Bachelor of Science Degree in Electrical Engineering from Oklahoma State University in December 2005. Completed the requirements for the Master of Science degree with a major in Electrical Engineering at Oklahoma State University in December, 2007.

Experience: Research Assistant for Dr. Keith Teague at Oklahoma State University from January 2005 through December 2007; intern Naval Research Laboratory during the summer of 2006 and 2007.

Professional Memberships: Institute of Electrical and Electronics Engineers

Name: Kellen Mitchell Harwell Date of Degree: May 2008

Institution: Oklahoma State University Location: Stillwater, OK

Title of Study: A COMPARISON OF 802.11 WIRELESS TRANSMITTER LOCALIZATION TECHNIQUES

Pages in Study: 99 Candidate for the Degree of Master of Science

Major Field: Electrical Engineering

Scope and Method of Study: The presence of an unsecured 802.11 access point is a major information security threat to government and business organizations. Thus it is necessary to accurately identify and isolate these devices. The purpose of this study is to evaluate various collection techniques used to geographically locate these unsecured access points. Using low cost hardware to passively capture data, a comparison is made between the use of omnidirectional and directional antennas. Stationary as well as mobile collections are performed for each of these antenna types. Various propagation models and estimation algorithms are compared to determine which method provides the most accurate results over varying and uncertain wireless environments.

Findings and Conclusions: Testing methods utilizing directional antennas exhibited very accurate results for a range of collection environments. Even in the presence of severe multipath, the analysis techniques were able to identify these reflections and compensate.

.

The methods employing omnidirectional antennas, however, produced inconsistent overall results. While the propagation model estimates were accurate for some sites, they were highly inaccurate for others. Due to the varying environment types that are encountered during wireless data collection, the use of generalized propagation models to provide source location is unreliable.

ADVISER'S APPROVAL: _____